Australian Government | acma

Australian Communications and Media Authority

An overview of international cyber-security awareness raising and educational initiatives

Research report commissioned by the Australian Communications and Media Authority

MAY 2011

communicating | facilitating | regulating

Canberra
Purple Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 44
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899
TTY 03 9963 6948

Sydney
Level 15 Tower 1
Darling Park
201 Sussex Street
Sydney NSW

PO Box Q500
Queen Victoria Building
Sydney NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799

Published by the Australian Communications and Media Authority

galexia

An Overview of International Cyber-Security Awareness Raising and Educational Initiatives

Authors:

Chris Connolly

Alana Maurushat

David Vaile

Peter van Dijk

Additional research:

Stephanie Cuevas

Melissa Wong

2011

A Galexia research report, with assistance from the Cyberspace Law and Policy Centre at the University of New South Wales – commissioned and funded by the Australian Communications and Media Authority (ACMA)

www.galexia.com

Cyberspace Law and Policy Centre

Contents

1. Executive Summary

Galexia <www.galexia.com.au> was commissioned to provide the Australian Communications and Media Authority (ACMA) with a comparative study of international Cyber-Security awareness raising and educational initiatives. Galexia has prepared this report with the assistance of the Cyberspace Law and Policy Centre <www.cyberlawcentre.org> at the University of NSW.

1.1. Methodology

This project has consisted of two research components:

— **Component 1 – Comparative analysis of international initiatives**
The first component was a comparative analysis of the approaches taken internationally to provide awareness raising and educational activities designed to empower the general and small business community with respect to Cyber-Security risks. This study examined a selection (68 in total) of initiatives in 11 jurisdictions. This study is not intended to represent an exhaustive study of every initiative in every jurisdiction. There has been a focus on English language initiatives – although 13 French and German initiatives were included in the study. Australian initiatives and resources were not included in this study.

— **Component 2 – Campaign evaluations**
The second component was an analysis of the literature used to support the implementation of these strategies as well as literature that evaluates the effectiveness of Cyber-Security education and awareness raising programs. This involved the examination of the only 2 initiatives (out of 68) where an evaluation had been conducted – plus 5 evaluations of similar campaigns in other fields (such as cyber-safety). This study is reporting on evaluations that are available and not evaluating campaigns per se.

1.2. Key Findings – Component 1 – International initiatives

Component 1 of the research found that a diverse range of education and awareness campaigns have been conducted on Cyber-Security issues. This report examined 68 international initiatives (these are the subject of detailed review in *Appendix 1 – International Campaigns* at page 24).

The research included a comparative analysis of these campaigns (refer to *Chapter 2 – Comparative analysis of international initiatives* at page 8).

Key findings concerning international initiatives include:

— The dominant tools used in most campaigns were basic web sites and publications. The proportion of campaigns employing interactive tools such as games and quizzes was quite low. Also, the proportion of campaigns that included a reporting or counselling service was very low;

— Government organisations (either departments or regulators) were the dominant 'host' of the campaigns, although consortiums that included the private sector were also common. A smaller number of campaigns were hosted by the community sector;

— The topics covered in the campaigns were quite diverse – no single topic appeared in a majority of campaigns;

— There are some gaps in the content provided in the education programs identified in this study;

— The target audience for campaigns included in this study was also quite diverse – no single target group dominated and many of the campaigns targeted multiple groups; and

— Information on the cost of campaigns was difficult to acquire – out of the 68 programs included in the study, 4 programs disclosed budget information.

1.3. Key Findings – Component 2 – Campaign evaluations

This component examined the only 2 initiatives (out of 68) where an evaluation had been conducted – plus 5 evaluations of similar campaigns in other fields (such as cyber-safety). This study is reporting on evaluations that are available and not evaluating campaigns per se.

This component of the research displayed that the number of public evaluations of campaigns, as a proportion of the number of campaigns conducted, appears to be low. As many Cyber-Security education and training initiatives are relatively new, a consensus as to the most effective initiatives has not yet emerged.

Many good practices, however, are being formed with some encouraging (although limited) evaluation results. Some useful lessons can be gained from an examination of the limited evaluations that are available.

Key findings concerning campaign evaluations include:

— The evaluations highlight problems in developing Cyber-Security education and training campaigns that are both appropriate *and* cost-effective;

— Host organisations find it challenging to evaluate the effectiveness of education and training initiatives – qualitative and quantitative metrics are difficult to put into place for such initiatives;

— The most reliable evaluations of projects have involved a multi-process method whereby key performance indicators and metrics are in place before, during and after the project;

— Many projects falsely assume that if a user acquires more information on Cyber-Security that this will automatically translate to more secure conduct online. The research demonstrates that this is not necessarily so. Websites, leaflets and other information-only style projects will have a limited impact if not followed with hands-on skills acquisition;

— Where a project is information-only, television advertisements have been proven most effective in message dissemination;

— The most successful projects are ones that integrate information with training and skill acquisition. Skill acquisition may take place through formal training programs, online quizzes, video games, and formal curriculum assessment; and

— Many organisations have found the most cost-effective way to produce positive results is to keep a project simple and focused on a target group.

1.4. Recommendations

This report makes some recommendations for organisations in Australia, based on a combination of the findings in Component 1 and Component 2. The recommendations are:

— **Recommendation 1: Evaluation**
The establishment of an evaluation framework for Cyber-Security education and awareness campaigns in Australia.
(Details of the proposed framework are included in *Section 4.1* at page 22)

— **Recommendation 2: Criteria for effective campaigns**
The development of a set of criteria for commissioning and evaluating Cyber-Security education and awareness campaigns in Australia.
(Details of the proposed criteria are included in *Section 4.2* at page 22)

— **Recommendation 3: Coordination**
Improved coordination of Cyber-Security education and awareness raising campaigns in Australia.
(Details of the proposed coordination steps are included in *Section 4.3* at page 23)

— **Recommendation 4: Further Research**
Further research in two key areas of Cyber-Security education and awareness raising campaigns.
(Details of the proposed research are included in *Section 4.4* at page 23)

2. Component 1 – Comparative analysis of international initiatives

2.1. Methodology

The first component of this research project was a comparative analysis of international approaches to provide awareness raising and educational activities designed to empower the general and small business community with respect to Cyber-Security risks. This section provides a broad overview of some of the key trends identified in our study of 68 international campaigns (more details are provided *in Appendix 1 – International Campaigns* at page 24).

This study examined a selection (68 in total) of initiatives in 11 jurisdictions. This study is not intended to represent an exhaustive study of every initiative in every jurisdiction. There has been a focus on English language initiatives – although 13 French and German initiatives were included in the study. Australian initiatives and resources were not included in this study.

Jurisdiction	Number of campaigns studied
International campaigns (page 24)	5
Canada (page 30)	5
France (page 35)	8
Germany (page 42)	6
Hong Kong (page 48)	2
Ireland (page 53)	3
Japan (page 56)	1
Korea (page 57)	1
New Zealand (page 58)	9
Singapore (page 67)	4
United Kingdom (page 71)	4
United States (page 75)	20
Total:	**68**

This component of the study was based upon a desk review of online resources. The research team also contacted key individuals in a number of the campaigns to validate the information collected.

Each campaign was examined using a common analysis template. The key criteria were:

- Campaign Name
- Organisation
- Main URL
- Dates
- Costs
- Topics covered
- Target Audience
- Methodology (Campaign Tools)
- Evaluation
- Additional Information
- Sources

2.2. Campaign tools

The campaigns included in this study employed a wide variety of campaign tools. However, as displayed in the following table, the most common tools were basic web sites and publications. The proportion of campaigns employing interactive tools (such as games and quizzes) was quite low. Also, the proportion of campaigns that included a reporting or counselling service was very low.

As can be seen in the summary table, many campaigns used more than one tool:

Campaign tools	Total number of campaign tools	% of campaign tools total	% of campaigns (out of 68)
Web site	68	34%	100%
Publications	23	11%	34%
Awareness Day/Week/Month	19	9%	28%
Training Seminars / Guidebooks	19	9%	28%
Videos	17	8%	25%
Games/Quiz	16	8%	24%
Hand-outs	15	7%	22%
Quiz	11	5%	16%
Report Service / Counselling	7	3%	10%
Software	4	2%	6%
Blogs	3	1%	4%
Total:	**202**		

This analysis may lead to some concern about the effectiveness of many of the campaigns. The limited number of campaign evaluations that have been conducted (refer to *Section 3.2 Campaign Evaluations* at page 13) include some cases where the provision of basic websites and publications was found to be an inefficient use of resources, especially when compared to more interactive campaigns that have focussed on skills acquisition.

The analysis also notes that nearly 28% of initiatives include an *Awareness day/week/month*. There may be some concern about the value of these *Awareness days/weeks/months* if they occur on different dates (both within and across jurisdictions), and if they do not include a practical activity for the target audience.

2.3. Host organisation

The campaigns included in this study were hosted by a wide variety of organisations. Most campaigns included a Government host (either a regulator or a relevant Government department). However, it was common for the Government host to be part of a consortium, including private sector or non-profit partners.

Collaboration with the industry sector can bring significant skills, profile, reach and financial resources to the campaigns. However, there may be cause for concern in campaigns where private sector branding is prominent – this may lead to perception of conflicts of interest and/or send an inconsistent message to consumers.

Involvement of the community sector potentially improves trust and confidence in the message, and may also help in reaching difficult / vulnerable audiences.

Host Organisation	Total number of campaigns	% of campaigns (out of 68)
Consortium	17	25%
Government (Regulator)	16	24%
Government (Department)	11	16%
Non-profit	9	13%
Other	16	22%
Total:	**69**	

2.4. Content

The content included in the campaigns was quite diverse. Many campaigns covered multiple topics, but no single topic appeared in a majority of campaigns.

Topics covered	Total number of topics	% of topics total	% of campaigns (out of 68)
Internet Safety	26	13%	38%
Privacy	19	10%	28%
Fraud	19	10%	28%
Phishing	15	8%	22%
Malware	15	8%	22%
Identity Theft	13	7%	19%
Spam	12	6%	18%
Firewalls	10	5%	15%
Passwords	10	5%	15%
Cyber Bullying & Harassment	11	6%	16%
Shopping	9	5%	13%
Business	8	4%	12%
Other	28	14%	41%
Total:	**195**		

Based upon the limited samples and jurisdiction examined in this study, some gaps in campaign content have been noted. For example, there has been limited attention directed to the prevention of spam and address harvesting. Also, there were no programs that educate users on Botnets. Governments and security experts have identified Botnets as a significant threat to the Internet.

2.5. Target audience

The target audience for campaigns included in this study were also quite diverse. 30% of the campaigns targeted general consumers and did not focus on any particular category of consumer. Many campaigns targeted multiple groups (an average of 3 groups were targeted in each campaign). However, no specific group was targeted by more than 12% of the campaigns.

Target audience	Total number of audiences	% of audiences total	% of campaigns (out of 68)
Consumers	48	30%	71%
Children	19	12%	28%
Small Business	18	11%	26%
Young people	18	11%	26%
Parents	14	9%	21%
Teachers	11	7%	16%
Government Employees	10	6%	15%
Elderly	8	5%	12%
IT Specialists	8	5%	12%
Non-profit Organisations	4	2%	6%
Vulnerable group	3	2%	4%
Total:	**161**		

Some target groups may be difficult to reach – for example small businesses and vulnerable and disadvantaged consumers. Each target group has communication/learning attributes that may require a change in style or method of delivery – a model of a single un-differentiated general audience is unlikely to shape projects that meet the needs of *any* group.

Different target groups may also face different risks or hazards to which they are more prone, so the content of campaigns may also have to change to meet the needs of specific groups. Education efforts need to be informed by research identifying these specific vulnerabilities, and to a considerable extent aimed at them. The option of a large range of generic offerings may not be the most effective mode to reach the more difficult less engaged groups.

2.6. Costs

Information on the cost of campaigns was difficult to acquire – out of the 68 programs included in the study, 4 programs disclosed budget information.

The following table summarises the limited public information that is available about campaign costs.

Campaign Costs	Total cost	Period that costs apply to
France – Campaign 8 – f@mily en ligne (family online) (page 41)	1 million euro	1 year
Germany – Campaign 1 – BSI (German Federal Office of Information Technology Security) (page 42)	222,038 euro	4 years
Ireland – Campaign 1 – Research Information Technologies – Centre for Secure Information Technologies (CSIT) (page 53)	30 million pounds	5 years
United States – Campaign 1 – National Cyber-Security Alliance (2001) (page 75)	3.75 million USD	3 years

This data is insufficient to enable a proper consideration of costs, benefits and return on investment for these campaigns.

Evaluations (which are already very limited) tend to overlook value-for-money criteria, and do not appear to consider how many consumers are 'reached' by each campaign (nor are targets set for this criteria). In other areas of education and awareness raising this would be considered critical.

3. Component 2 – Evaluation of campaigns

3.1. Methodology

The second component of this research report is an analysis of the literature used to support the implementation of Cyber-Security education and awareness raising campaigns, as well as literature that evaluates the effectiveness of such campaigns.

This component examined the only 2 initiatives (out of 68) where an evaluation had been conducted – plus 5 evaluations of similar campaigns in other fields (such as cyber-safety). This study is reporting on evaluations that are available and not evaluating campaigns per se.

A significant challenge in reviewing the effectiveness of Cyber-Security campaigns is that there have been few evaluations, either quantitative or qualitative, for the campaigns. Although 68 campaigns were examined in Component 1 of this report, only 2 of those campaigns were the subject of a public independent evaluation (*MakeIT Secure*[1] in Ireland and *Family Online*[2] in France). The other 5 evaluations are therefore based on available resources that evaluate generic IT security campaigns or cyber-safety campaigns. These topics are considered compatible with Cyber-Security campaigns and still provide useful lessons.

3.2. Campaign Evaluations

A significant challenge in reviewing the effectiveness of Cyber-Security campaigns is that there have been few evaluations, either quantitative or qualitative, for the campaigns. The design of the campaigns may be such that evaluation only occurs at the end of the campaign. Many of the campaigns have been recently initiated such that there may not have been the opportunity for evaluation. Evaluations may also have occurred but not been publicly disclosed.

The following campaigns, therefore, have been selected due to the fact that there has been an evaluation of the campaign. The inclusion of extra detail on these campaigns is not meant to imply any support for these campaigns or to indicate that they are more worthy of study than the other campaigns listed in *Appendix 1 – International Campaigns* at page 24. They are being analysed in more detail simply because they include evaluations, and the evaluations provide useful lessons for Australia.

[1] *Refer to Section 3.2 – Campaign B. An evaluation of the MakeITsecure campaign* at page *15.*

[2] Refer to *Section 3.2 – Campaign A. F@milie en ligne: Sur internet, la securité ça commence aussi par vous (Family Online: Internet Security Begins With You)* at page 14.

A. F@milie en ligne: Sur internet, la securité ça commence aussi par vous (Family Online: Internet Security Begins With You)

Refer to *Appendix 1: France: Campaign 8 – f@mily en ligne (family online)* at page 41.

Abstract: In May 2006, the French Ministry of the Family launched an information security-awareness campaign informing parents of the potential risks to which minors are exposed while surfing on the Internet and to make them aware on how to use the Internet. As part of the F@mile en ligne programme, the ministry broadcast a series of 10 films. These films show the Internet experiments of a family and its knowledge on various existing security solutions. Each 45-second episode was broadcast twice on the two most popular channels for children and young people in France (TF1 and M6) between 15 May and 2 June 2006.

Methodology: An independent evaluator carried out surveys with over 1000 parents and their children (aged 11 to 17) prior to the launch of the film campaign assessing parental knowledge of their children's Internet use compared with their children's *actual* use of the Internet. After the film campaign another independent assessment was done via a survey, which examined a number of components.

Findings: There were some pertinent findings from the surveys:

- 59% of the parents with an Internet connection at home have heard of, read of or have seen an information awareness-raising campaign to inform parents of the potential risks to which minors are exposed while surfing on the Internet and to make them aware of how to use the Internet; 37% had not heard of the campaign;
- 84% watched one of the 10 films at least once and declared that they liked them;
- 92% liked the title and message of the campaign;
- 98% estimated that the films are necessary to raise awareness of information security, 94% could identify the characters of the films with people they know; and
- 71% indicated that the campaign raised awareness of the risks encountered while using the Internet

B. An evaluation of the MakeITsecure campaign

A public/private initiative aimed at a television campaign and comprehensive website known as makeITsecure.ie. Refer to *Appendix 1: Ireland: Campaign 3 – MakeITsecure* at page 55.

> **Abstract:** The Department of Communication, Marine and Natural Resources together with BT, Dell, Eircom, the Irish Bankers Federation, IAB, Microsoft, Symantec, the National Centre for Technology in Education, Ward Solutions and Vodafone are working together to raise awareness of the urgent need for consumers and businesses to make their computer secure. This public-private consortium has created the second national computer security awareness campaign: 'makeITsecure'. The growth in PC ownership and availability to children, the increased use of online banking, the increased volume spam, Internet access and usage and the current broadband levels of over 15% of the population are some of the reasons why the consortium has launched the second edition of this initiative. The 2005/2006 campaign addressed emerging issues, such as' Phishing; identity theft; spyware and child safety online.
>
> **Methodology:** A survey was used to document pre-campaign awareness versus post-campaign awareness.
>
> **Findings:** Awareness increased to 44% (from 33% in 2004). Security measures taken by Internet users all increased. Over half of 'aware' users undertook extra PC security measures as a result of the campaign. Understanding of terms such as 'identity theft' and 'spyware' improved dramatically in the post-2005 campaign research with scores of 55% (from 24% pre-campaign) and 49% respectively (from19%).

C. An Analysis of Electronic Media to Prepare Children for Safe and Ethical Practices in Digital Environments

Berson, I.R., Berson, M.J., Desai, S., Falls, D., & Fenaughty, J. (2008). 'An analysis of electronic media to prepare children for safe and ethical practices in digital environments'. *Contemporary Issues in Technology and Teacher Education* [Online serial], *8*(3). <http://www.citejournal.org/vol8/iss3/socialstudies/article2.cfm>

> **Abstract:** A range of electronic resources, including video–based instruction, is used to promote cybersafety to young people at school. This evaluation analysed seven distinct programs that use electronic media in Internet safety initiatives in schools. The findings highlight emerging evidence on successful approaches to engage children in assessing risky cybersafety situations, developing appropriate management techniques, and practicing responsible decision making online. Based on the prevention effectiveness literature and the tenets of behaviour decision theory, a rubric was developed to evaluate the effectiveness of online instructional materials in teaching ethical behaviour in digital environments. The rubric demonstrates that high quality cybersafety resources are based on a coherent theoretical framework, integrate multiple program components, and allow for skill rehearsal.
>
> **Methodology:** The authors of the evaluation consist of university researchers specialising in early childhood education, a teacher and a representative from New Zealand's NetSafe Internet Safety Group. Seven electronic resources using video-based instruction were evaluated using a six-factor grid. The electronic resources were: BrainPop-Computer Viruses, Disney Surf Swell Island, Hector's World, iKeepsafe, iSafe, Media Aware and Netsmartz. There were two undisclosed reviewers for each electronic resource rating the following factors:
>
> 1) Based on a coherent theoretical framework,
>
> 2) Includes active, systematic and specific skill training,
>
> 3) Integrates multiple program components (i.e., classroom training combined with parent involvement),
>
> 4) Includes interactive instructional techniques,
>
> 5) Provides intensive training, and

6) Addresses protective factors as well as risk factors.

Findings: The assessors found that sites which made the assumption that increased knowledge would result in better choices had the less favourable reviews. Sites, however, which were based on theoretical approaches based on critical components that would change children's behaviour were reviewed more favourably. Hector's World had the best reviews of all of the resources evaluated.

D. Implementing an Integrated National Cybersafety Programme for the Compulsory School Sector

'Implementing an Integrated National Cybersafety Programme for the Compulsory School Sector' Douglas Harré, Senior ICT Consultant, Ministry of Education, Wellington, New Zealand. <http://www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/douglas_harre.pdf>

Abstract: Keeping students safe in an increasingly pervasive digital environment has been a challenge for many jurisdictions around the world. This task is usually undertaken by one or more relevant government departments within a country. Since 1999 the Ministry of Education in New Zealand has funded the provision of a range of cybersafety initiatives that have resulted in a comprehensive, integrated approach to this issue.

Methodology: A government consultant has provided two case studies of government programs. The first case study, entitled Managed Internet Service Project, essentially is a program that gives filtering and monitoring products to schools for free. The second case study, Forensics Audits, involves randomly auditing selected New Zealand schools to assess whether the schools' computers were storing any objectionable materials (calendar style pictures, jokes, naked images, hardcore pornography, and objectionable images).

Findings: Statistics are provided for each case study such as the percentage of schools with images of hardcore pornography.

E. A Perspective on Achieving Information Security Awareness

'A Perspective on Achieving Information Security Awareness', Mariana Hentea, Southwestern Oklahoma State University, Weatherford, USA.
<http://proceedings.informingscience.org/InSITE2005/I14f89Hent.pdf>

> **Abstract:** The guidelines 'Towards a Culture of Security' emphasise a culture of security in all aspects of information systems, from designing and planning through to everyday use, and among all participants, from government down through business to consumers. In response to national needs, Information Security education has become a priority for many educational institutions in US for the past years. More universities and colleges have established courses or specialized programs to teach Information Security skills to students enrolled in degrees related to computers such as computer information systems, computer engineering, and computer science. However, there are aspects of the security education model that need attention. This paper discusses these issues including changes to improve security awareness education. Through close coordination between faculty, industry, government agencies, and universities, the critical education of future graduates, Information Technology professionals, Information Security professionals, and public can be accelerated.
>
> **Methodology:** This evaluation is a literature review of studies in information security education and training. The thesis of this evaluation is that education and training initiatives should be used for training in post-secondary education of computer programmers. Of those initiatives currently being used, more emphasis should be placed on skills in designing programs.

F. Evaluation of the Block Bullying Online Campaign 2009

'Evaluation of the Block Bullying Online Campaign 2009', DG Information Society and Media, Final Report, August 2009. <http://ec.europa.eu/information_society/activities/sip/docs/report_bullying.pdf>

> **Abstract:** In February 2009 the European Commission, together with the INSAFE network, launched a pan – European communication Campaign on Safer Internet and in particular cyber bullying which was developed by the Safer Internet Programme[1]. The name given to the Campaign was 'Internet is fun. Keep it fun, keep control! Block Bullying Online!'. This report is an evaluation of that campaign.
>
> **Methodology:** The methodological approach taken by the independent evaluators consisted of desk based review of key documentation, familiarisation interviews with key stakeholders, six focus groups across three countries, omnibus panel surveys with the target group aged 16 and 17 in three countries, online surveys with the target group aged 12 to 17 in five languages, and a media monitoring template to record information on the reach of dissemination activities.
>
> **Findings:** Although the campaign was on cyber-bullying, rather than cyber-safety, it is one of the few reports of an independent evaluation with excellent methodology, so it has much relevance here. For example:
>
> > **Key lesson 3:** TV has been clearly identified through the evaluation evidence as the key medium for communication. Any future Campaign should build on and grow the contacts made so far. (TV stations were persuaded to provide free airtime or broadcasting discounts).
> >
> > **Key lesson 4:** Any campaign material that is developed needs to have several dimensions.
> >
> > **Key lesson 5:** There needs to be a wider range of feedback from the target group in a larger number of countries at *the earliest stage* of the campaign's development.

G. Information Security Awareness: Local Government and Internet Service Providers

ENISA (The European Network of Information Security Agency) report on 'Information Security Awareness: Local Government and Internet Service Providers' (2007) <http://www.enisa.europa.eu/act/ar/deliverables/2007/loc=gov/en>.

Abstract: This report details the information security awareness programmes undertaken by government (national and/or local) with an outreach to Internet service providers (ISPs). These initiatives represent government and ISP efforts to promote and develop a 'culture of security' among users within the European Member States.

Methodology: The research was carried out using a survey, which was made available to the European Internet Services Providers Association (EurolISPA), The European Local Authorities' Telematic Network (Elanet), Eurocities and their members.

Findings: This report offers a series of Cyber-Security initiatives from various European countries along with evaluations of the studies. Because of the limited sample size, the report offers an analysis of the findings and their commonalities without a study of the European trends in this field. The main findings are as follows:

- Information security is seen as a high priority by local government and ISPs;
- The level of knowledge of the target groups is fairly limited or generally low;
- Most of the organisations and public bodies plan, organise and deliver information security awareness initiatives for a period of at least 12 months;
- Within local government organisations, information security awareness-raising activities are often part of a larger ICT campaign;
- Training is considered the most effective technique. Setting out comprehensive computer-based training plans and communication tools can help train employees to ensure programme effectiveness;
- Public-private partnerships can be a highly effective means of delivering campaigns, especially if each organisation can use their respective strengths and mobilise appropriate resources;
- The importance of measuring the effectiveness of information security awareness of programmes is duly recognised.

3.3. Challenges for Evaluation

The limited number of evaluations is a useful indicator that organisations face significant challenges in conducting evaluations of Cyber-Security education campaigns. There is no direct literature explaining why so few evaluations have been undertaken, but some challenges can be identified from the comparative analysis of the campaigns:

— The design of the campaigns may be such that evaluation only occurs at the end of the campaign. Many of the campaigns have been recently initiated such that there may not have been the opportunity for evaluation;

— Evaluation may have occurred but has not been publicly disclosed;

— Qualitative and quantitative metrics[3] are difficult to put into place for the evaluation of training and awareness initiatives (in any sector); and

— Project budgets may not have included an evaluation component – and evaluation can be and expensive undertaking.

[3] Examples of metrics include:
- Consumer surveys to measure awareness before and after campaigns
- Analysis of website traffic
- Analysis of skills acquisition before & after campaigns

There are also challenges in determining 'when' to evaluate a campaign. Post-project 'program evaluation' is useful and required, but may be too late and 'after the fact' to have an impact on current projects. Evaluation after the project may offer some guidance for design of new projects, but it will be too late to assist the now completed project.

The most reliable evaluations of projects have involved a multi-process method whereby key performance indicators and metrics are in place before, during and after the project. The French project *Family Online* is a good example of multi-process metrics [Refer to *Section 3.2 Campaign Evaluations: A. F@milie en ligne: Sur internet, la securité ça commence aussi par vous (Family Online: Internet Security Begins With You)* at page 14].

Another perspective on when to evaluate is drawn from software development methodology, and its use of 'work in progress' evaluation throughout a project to address the high failure rate of large software projects. This integrates evaluation, particularly of alignment with well understood user needs, into the design process, not just the program governance and review stage, and thereby offers a technique for assisting new and current projects. See below at the end of this chapter for further discussion.

3.4. Campaign tools – Inclusion of skills acquisition

One of the key lessons from both Component 1 and Component 2 of this research report is that a diverse range of campaign tools has been used to date, without necessarily being the most effective use of resources.

The evaluations provide support for the use of interactive campaign tools that promote skills acquisition and rehearsal of those skills. This may require a mix of both information-only campaign tools (such as general website information and publications) and interactive tools.

Many projects assume that if a user acquires more information on Cyber-Security then this will automatically translate to more secure conduct online. Some campaigns therefore focus on the provision of ever-growing website information and publications. However, the evaluations demonstrate that this is not necessarily the most effective approach. Websites, leaflets and other information-only style projects will have a limited impact if not followed with hands-on skills acquisition.

The more successful projects appear to be those that integrate information with training and skill acquisition. Skill acquisition may take place through formal training programs, online quizzes, video games, and formal curriculum assessment.

For children and young people in particular, information probably needs to be complemented by an activity that allows them to 'rehearse' their skills (games, quizzes, virtual reality etc.).

3.5. Campaign tools – Inclusion of a reporting function

There are clear benefits realised from incorporating practical measures and 'reporting' functionality into Cyber-Security education and awareness raising campaigns – so that there is a greater link between the education of consumers and subsequent action. Can consumers who are engaged by the education campaign take immediate practical steps to improve their Cyber-Security? If they become aware of a Cyber-Security risk how can they report it?

Incorporating a tool for reporting security incidents or abuse may be useful -- otherwise consumers feel powerless, or that they carry the entire burden of Cyber-Security, and this may erode confidence in the use of online communications and Internet technology generally.

3.6. Campaign tools – The continuing power of television

It may seem strange in a report on Cyber-Security to highlight the potential use of television as an education and awareness raising tool, but several of the evaluations pointed to the continuing power of television as a mechanism for reaching target audiences and delivering a clear and memorable message.

Where a project is information-only, television advertisements have been proven most effective in message dissemination. See for example the French *f@mily en ligne* project
[Refer to *Section 3.2 Campaign Evaluations: A. F@milie en ligne: Sur internet, la securité ça commence aussi par vous (Family Online: Internet Security Begins With You)* at page 14]

The *European Evaluation of the Block Bullying Online Campaign 2009* reached a similar conclusion:

> **Key lesson 3:** TV has been clearly identified through the evaluation evidence as the key medium for communication. Any future Campaign should build on and grow the contacts made so far. (TV stations were persuaded to provide free airtime or broadcasting discounts).[4]

Note however that although this study has found that television is an effective medium for the delivery of information-only style campaigns, the study has also cautioned against over-reliance on such campaigns. This report supports a focus on interactive resources such as quizzes, games and virtual reality tools.

3.7. Target audience – Focussed campaigns

One approach to delivering a cost-effective campaign with positive results is to ensure the project is simple and focused on a target group. This does not, however, mean that a project should be one-dimensional. The information should be simple with education and training delivered in a multi-dimensional manner.

For example, a project could commence with targeted television advertisements and be followed up with an education and training mechanism – delivered during this time by multiple organisations (both public and private). This may include mechanisms such as YouTube clips, online video games, and a security awareness month. The use of multipliers (multiple tools and channels within the one campaign) has the effect of rapid and widespread dissemination.

3.8. Cost effectiveness

None of the 7 evaluations consider cost effectiveness in any detail. Where costs were noted in campaigns (4 out of 68 campaigns examined in Component 1 of this study disclosed costs), they appear high. Refer to *Section 2.6 Costs* at page 12.

This makes is difficult to identify Cyber-Security education and training campaigns that are cost-effective. This lack of data may be a barrier to the development of effective future campaigns.

3.9. 'Work in progress' evaluation, as part of the design process

Established disciplines in software and web development methodology use 'work in progress' evaluation throughout a project to address the high failure rate of large software projects (which some online services resemble).[5] Core techniques include 'iterative development' and 'software prototyping' conducted to generate interim design artefacts for users and others to evaluate. The aim is to integrate evaluation into the design process, and thereby improve fitness for the needs of users. Rather than evaluation as traditional after-the-fact assessment of program success or failure, this puts ongoing evaluation of progress towards understanding and resolution of risks, and in particular towards satisfaction of known user needs, at the heart of the development process. It promises not only greater visibility of progress, but also delivery of materials actually useful to known users.

---

[4] Evaluation of the Block Bullying Online Campaign 2009, DG Information Society and Media, Final Report, August 2009. <http://ec.europa.eu/information_society/activities/sip/docs/report_bullying.pdf>

[5] For instance, the extensive literature starting with McConnell S (1996) *Rapid Development: taming wild development schedules*, Microsoft Press, especially Ch. 7 and spiral life cycle model; Mayhew J (1999) *The Usability Engineering Lifecycle: practitioner's handbook for user interface design;* Pearrow M, (2000) *Web Site Usability Handbook*, Charles River Media, esp. Ch 2.

This approach relies on frequent 'work in progress' evaluation of the developers' understanding of, and progress towards, goals. It is a central technique to steer current projects towards outputs better aligned with demonstrated needs of identified groups of users. It is based on a gradually elaborated set of sketches, prototypes and disposable artefacts representing current thinking about the nature of 'the problem' and the shape of 'the solution'. The goal is to make the designers' thinking and assumptions visible to a wide range of users and user surrogates from the very earliest, feasibility assessment stages of the project, and to use them to prompt user and other feedback to reveal errors in assumptions, language or plans at the earliest possible time. Early discovery means remediation is cheap and effective, while discovery at the end means it is too late, expensive and difficult to use evaluation feedback in the project.

This model, which we recommend for routine adoption, also depends on sophisticated project managers and clients, willing to allow these user-centred evaluations to guide the scope, quality and content of the deliverables as the project evolves, and to reward rather than punish designers for focusing on 'making the worst mistakes early and visibly'. These can present challenges, albeit ones worth the effort.

4. Recommendations

4.1. Evaluation

The absence of campaign evaluations in the Cyber-Security education field should send a warning to any organisation considering conducting or supporting such campaigns. A large number of campaigns have been undertaken, subject to very limited evaluation or even discussion of their effectiveness.

This report recommends the establishment of an evaluation framework for Cyber-Security education and awareness campaigns in Australia. The best-practice approach to campaign evaluation may include the following:

— **1.** Promotion of independent and expert oversight for campaigns;

— **2.** The incorporation of an evaluation component into campaign budgets;

— **3.** The use of multi-process evaluations where key performance indicators and metrics are in place before, during and after each campaign;

— **4.** The integration of user-centred design evaluation techniques into all stages of the design process, to improve alignment with actual needs as a project develops;

— **5.** The publication of campaign evaluations so that key lessons can be shared; and

— **6.** The development and continuous refinement of design criteria for effective campaigns (refer to the following recommendation for further details).

4.2. Criteria for effective campaigns

It may be useful to develop a set of criteria for commissioning and designing campaigns in Australia. These criteria could be used to help direct limited resources towards campaigns that will be more effective and efficient.

Design criteria that may be appropriate in Australia (incorporating findings from this study) include:

— **1.** Campaigns should be based on a coherent education or awareness raising methodology;

— **2.** Campaigns should include active, systematic and specific skill training;

— **3.** Campaigns should integrate multiple program components;

— **4.** Campaigns should include interactive instructional techniques;

— **5.** Campaigns should incorporate practical activities and tasks that users can undertake to enhance Cyber-Security;

— **6.** Campaigns should, where possible, include a 'reporting' function that allows consumers to report Cyber-Security risks and incidents; and

— **7.** Campaigns should include a mix of comprehensive, long-term education and awareness raising – complemented by short and specific initiatives (micro-campaigns), where appropriate.

A similar set of criteria was developed and proposed by Berson and others in 2008 for cyber-safety campaigns[6].These can complement understanding of the detailed needs of a particular project's specific user groups which is generated by 'work in progress' evaluation techniques mentioned above.

4.3. Coordination

The effectiveness of Cyber-Security education and awareness raising campaigns would be enhanced by some limited efforts in coordination. Based on the observation of international practice during Component 1 of this study, there is potential in Australia for organisations to pursue a wide range of relatively uncoordinated campaigns, of limited duration, effectiveness and investment in proper development process, and aimed at a grab bag of audiences, topics and interests.

This study is not suggesting that all campaigns should be closely coordinated, or that a single organisation should have sole responsibility for campaigns. However, some specific coordination would deliver benefits. Four specific areas could benefit from coordination:

— **1. Awareness Days/Weeks/Months**
This study identified a number of awareness raising campaigns that were based on special days/weeks/months. These efforts are not necessarily co-ordinated across jurisdictions and may be confusing for consumers who now operate in a global environment.

— **2. Gaps in content**
There may be a role for an organisation to anticipate and respond to emerging Cyber-Security issues and risks. Perhaps they could also help to identify providers who could address emerging issues.

— **3. Locating content**
The location of useful material is currently spread across many host organisations, so it may be difficult for many users to find information that is particularly suited to their specific interests. Relatively informal coordination and collaboration between various potential providers, aimed at re-focusing the provision of these materials to identified needs in ways that are most effective and convenient and findable for users, would be warranted, though a centralised and tightly coordinated process may not be as effective as something that works with traditional Internet collaborative models.

— **4. Sharing evaluation**
One organisation could take on the role of coordinating and disseminating information on the evaluation of campaigns. This is discussed in more detail above.

4.4. Further research

This study identified some gaps in the research and literature regarding Cyber-Security education and awareness raising campaigns.

The most obvious gap is the lack of information on evaluations and evaluation methodology (discussed in detail above). This includes traditional external program and campaign evaluation, and also the integration of 'work in progress' internal evaluation into the design process.[7]

However, another significant gap is that the literature examined does not address the specific needs of any target groups (other than some limited information on different age groups). There is very little information available regarding the Cyber-Security education needs (or suitable education tools) regarding other vulnerable groups differentiated by language, disability, income level, or other factors.

[6] Berson, I.R., Berson, M.J., Desai, S., Falls, D., & Fenaughty, J. (2008). An analysis of electronic media to prepare children for safe and ethical practices in digital environments. *Contemporary Issues in Technology and Teacher Education* [Online serial], *8*(3). <http://www.citejournal.org/vol8/iss3/socialstudies/article2.cfm>

[7] See McConnell, and Mayhew, above.

5. Appendix 1 – International Campaigns

5.1. International campaigns

Campaign 1 – Cyber Criminals Most Wanted

This website provides Internet users with a plethora of resources for Internet safety and news from countries around the world. Additionally, the site provides pictures of wanted cybercriminals, hijackers, and criminals in an effort to heighten awareness of cybercrime and criminals who have yet to be arrested. The site does not provide users with an overview of the site, or a mission statement.

Item	Notes
Campaign Name:	Cyber Criminals Most Wanted (International, rooted in US)
Organisation:	Cyber Criminals Most Wanted
Main URL:	http://www.ccmostwanted.com/
Dates:	Copyright 1999 – 2010
Costs:	Not mentioned
Topics covered:	– News Articles in regards to cyber crime (Around the World) – News 4 Specific Topics (wide variety of topics from online hackers stealing cash to facebook privacy policies) – Internet Safety Guide – Internet Shopping Guide – Cyber Stalking – Cyber Terrorism – Digital Divide – Electronic Disposal – Fraud – Hacking – Hoaxes – ID Theft – Netiquette – Privacy – Scams – Security – Spam – Spyware – Viruses and Infectors – References for: (cybercrime professionals, attorneys, law enforcement, advanced professional services, register LE cybercrime unites, register LE cybercrime USA precincts) – Find Cybercrime Professionals: (attorneys – global, attorneys – USA, expert witnesses, forensic specialists, investigators, LE Cybercrime Units – global, LE Cybercrime Units – USA, LE Cybercrime Precincts – USA, LE Cybercrime Precincts – global) – Laws (In the USA, International) – About this Website (Contact, Policies, Mission) (All available from the drop down menus in the left bar)
Target Audience:	– Internet Users – Corporate Users – Educators – Families – Kids – Parents – Seniors – Teens

Item	Notes
Methodology:	– Online interactive games – Training and Seminars – Advertisements for Internet Security software – List of open seminars regarding Cyber-Security throughout the US and in the UK – Free online scanners – Advertisements for books regarding Internet Safety – Online Literature from an accumulation of websites – Advertisements through Facebook – Directs users to the Internet Crime Report Center in US
Evaluation:	Not found
Sources:	1. 'Home' *Cyber Criminals Most Wanted* <http://www.ccmostwanted.com/> (accessed 15 June 2010).

Campaign 2 – EU Safer Internet Program

First launched in 1999, the 'Safer Internet Program' is designed to educate the European community about Internet security, with an emphasis on risks for young people. 'Young people, parents, carers and teachers must be informed of the potential risks that youngsters may encounter online. Fighting illegal and harmful content and conduct online should be a priority.'

The main objectives are 'to promote the safer use of the Internet and other communication technologies, particularly for children and young people, to educate users, particularly children, parents, carers, teachers and educators in this regard and to fight against illegal content and harmful conduct online.'

Item	Notes
Campaign Name:	EU 'Safer Internet Program'
Organisation:	Europe's Information Society
Main URL:	http://ec.europa.eu/information_society/activities/sip/index_en.htm
Dates:	2009 – 2013
Costs:	No details available
Topics covered:	– Illegal content – Harmful conduct (e.g. grooming and bullying) – Promoting a safer environment – Raising awareness
Target Audience:	Young people and children
Methodology:	– Community consultation on internet security issues – Funds Safe Internet Centres in the EU member nations, some run hotlines where users can find out more about internet security – Pan-European content filtering and content labelling Among others, projects such as: – 'CIRCAMP', encouraging international law enforcement cooperation – 'MAPAP' a project that measures and analyses the peer to peer activity against paedophile content – 'SIP – BENCH' study whose objective was to assess filtering software and services currently available in order to provide guidance to parents and educators.
Evaluation:	Not found
Additional Information:	The most recent topics for community consultation are: – Age verification, cross media rating and social networking (2008) – Online technologies for children (2007) – Child safety and mobile phone services (2006)
Sources:	1. 'Safer Internet Program: the main framework for European policy' *Europe's Information Society* <http://ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm> (accessed 24 June 2010). 2. 'Empowering and protecting children online' *European Commission Information Society and Media* <http://ec.europa.eu/information_society/doc/factsheets/018-safer-internet.pdf> (accessed 24 June 2010).

Campaign 3 – Safe and Secure Online

(ISC)² is a global, not-for-profit organisation with headquarters in the United States and offices in London, Hong Kong and Tokyo.

> 'Through our Safe and Secure Online Program, our member volunteers help children ages 11 – 14 learn how to protect themselves online. With support from Childnet International, a UK – based charity that aims to make the Internet a safe place for children, we began Safe and Secure Online in 2006 to address the gap in security advice that exists in children's safety outreach efforts.'

Item	Notes
Campaign Name:	(ISC)² Safe and Secure Online Program
Organisation:	(ISC)²
Main URL:	http://cyberexchange.isc2.org/safe-secure.aspx
Dates:	Copyright 2008 – 2010
Costs:	Not found
Topics covered:	Wide range, including: – Sexting – Cyber Predators – Application and website security – Information protection – Spyware – SPAM – Online shopping – Phishing – Malware – Passwords
Target Audience:	General public (communities and organisations) 'Safe and Secure' specifically for children ages 11 – 14
Methodology:	– Provide vendor – neutral education products – Career services – Gold Standard credentials to professionals – Security awareness tools available for public download from website (and also upload by members) – 'Safe and Secure' program relies on volunteers to present their materials not only online, but also to schools
Evaluation:	Not found
Additional Information:	In terms of the certifications, (ISC)² claim their 'credentials are essential to both individuals and employers for the seamless safety and protection of information assets and infrastructures.'
Sources:	1. 'About (ISC)²' *(ISC)² Cyber Exchange* <http://cyberexchange.isc2.org/aboutus-moreinfo.aspx> (accessed 24 June 2010).

Campaign 4 – Anti-Phishing Working Group

The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types.

Item	Notes
Campaign Name:	APWG Public Education Initiative
Organisation:	Anti-Phishing Working Group
Main URL:	http://www.antiphishing.org/
Dates:	Unknown
Costs:	Not available
Topics covered:	– Phishing – Muling
Target Audience:	Consumers and enterprises
Methodology:	– Identifies and organises most useful cybercrime education programs and makes them available to widest cohort possible – Phishing Education Landing Page Program – aims to 'instruct consumers on online safety at the 'most teachable moment': when they have just clicked on a link in a phishing communication.' Works through ISPs and anyone else who has control over a phishing page to redirect consumers to the APWG Landing Page instead of an error message. – Counter Muling project developing series of video podcasts. Broad media campaigns planned for the future.
Evaluation:	Not found
Sources:	1. 'APWG Public Education Initiative' *Anti-Phishing Working Group* <http://education.apwg.org/index.html> (accessed 24 June 2010).

Campaign 5 – Security Cartoon

This site provides an overview for Cyber-Security threats using cartoons. It presents an innovative approach to educating the public about personal safety on the Internet. The severity of risks involved in each topic is summarized in a short comic strip in an effort to gain attention of users.

Item	Notes
Campaign Name:	Security Cartoon
Organisation:	Security Cartoon
Main URL:	http://www.securitycartoon.com/
Dates:	Published October 1, 2007
Costs:	Not disclosed
Topics covered:	– Spoofing – Malware – Phishing – Pharming – Passwords – Politics – Fight Back
Target Audience:	– Consumers
Methodology:	(more a single resource than a campaign)
Evaluation:	Not found
Additional Information:	A brief overview of the organization: 'Drs. Sukamol Srikwan and Markus Jakobsson developed SecurityCartoon.com in 2006 as an approach to improve security awareness and understanding among typical Internet users. The material is supported by their insights into computer security, deceit psychology and learning. The approach has been documented in a recent scientific journal ('Using Cartoons to Teach Internet Security', Cryptologia, vol. 32, no. 2, 2008) and in a book chapter (chapter 13 of Crimeware, Symantec Press, 2008). In 2007, Srikwan and Jakobsson founded Extricatus, LLC, a Mountain View, CA company. Extricatus' charter is to improve security messaging and reduce security vulnerabilities due to social engineering and human error, two of the leading causes to security breaches. Among their clients are five Fortune-500 companies, and several European and Latin American companies concerned with the rising tides of online fraud.'
Sources:	1. 'Home' *Security Cartoon* <http://www.securitycartoon.com/> (accessed 23 June 2010). 2. 'About Us' *Security Cartoon* <http://www.securitycartoon.com/about.php> (accessed 23 June 2010).

5.2. Canada

Campaign 1 – Centre of Operations Linked to Telemarketing Fraud (COLT)

This site focuses on mass marketing fraud. 'The COLT mission is threefold: offer prevention and education programs, carry out interception operations and conduct mass marketing fraud investigations.' The education component includes general information about mass-market fraud, and information aimed at potential telemarketing employees. The latter material on the website was accompanied with a handout of flyers to students. Mass-market fraud investigations and education topics look at media including phones, mobile phones and Internet (including chat rooms, e-mails, payment system) as well more traditional postal methods, classifieds, fraudulent, lottery scams and prior frauds.

Item	Notes
Campaign Name:	COLT (Centre of Operations Linked to Telemarketing Fraud)
Organisation:	The Centre of Operations Linked to Telemarketing Fraud (COLT), a joint operation involving a range of Canadian and US law enforcement and regulatory agencies
Main URL:	http://www.rcmp-grc.gc.ca/qc/services/colt/telemarket-fraud-eng.htm
Dates:	1998 to present
Costs:	Not disclosed.
Topics covered:	Mass marketing fraud (telemarketing via phone, mobile phone, post and Internet)
Target Audience:	Consumers and potential employees (students)
Methodology:	Education of consumers and those likely to become victims. – Some general information on mass market scams with general advice on how to avoid becoming a victim – Public advertisement campaign through advertisements and flyers handed out to students (potential telemarketing employees) warning of the dangers of working for fraudulent businesses
Evaluation:	Not found
Additional Information:	In 1998, the RCMP Commercial Crime Section in Montreal launched an integrated project to combat mass marketing fraud. The Centre of Operations Linked to Telemarketing Fraud (COLT) is a joint forces operation involving the Royal Canadian Mounted Police (RCMP), *Sûreté du Québec* (*SQ*), City of Montréal Police Service (*SPVM*), Competition Bureau, Canada Border Services Agency (CBSA), Federal Bureau of Investigation (FBI), Department of Homeland Security (Immigration & Customs Enforcement), US Postal Inspection Service and US Federal Trade Commission. The COLT team also works in close cooperation with Canada Post, Canada Revenue Agency and the Canadian Anti-Fraud Call Centre (PhoneBusters). The COLT team is tasked with investigating mass marketing fraud operations based in the greater Montreal area. Through prevention and education programs, it also aims to be proactive in putting an end to fraudulent activities and raising public awareness about this type of crime.
Sources:	1. <http://www.rcmp-grc.gc.ca/qc/services/colt/telemarket-fraud-eng.htm> (accessed 23 June 2010).

Campaign 2 – PhoneBusters: The Canadian Anti-Fraud Centre, and SeniorBusters

The Canadian Anti-Fraud Centre's two main roles are educating the public about specific fraudulent schemes, and collecting and disseminating victim information, statistics and documentation to provide investigative assistance to law enforcement.

Item	Notes
Campaign Name:	PhoneBusters: The Canadian Anti-Fraud Centre, and SeniorBusters (for senior citizens)
Organisation:	The Canadian Anti-Fraud Centre
Main URL:	http://www.phonebusters.com/english/index.html
Dates:	1993 till present
Costs:	Not disclosed.
Topics covered:	Fraud scams (predominantly related on scams sent via spam)
Target Audience:	Consumers with particular focus on those most likely to become victims of scams, senior citizens (SeniorBuster)
Methodology:	Education of consumers and those most likely to become victims (often senior citizens). – Categorised scams (Eg. Puppy scams, lottery emails, advance-fee scams, phishing) – There are a number of examples of the exact texts of the scams so that users have concrete examples of current scams Consumers may report scams via telephone, fax or email
Evaluation:	Not found
Additional Information:	'Established in January of 1993, the Canadian Anti-Fraud Centre (formerly PhoneBusters) is jointly managed by the Royal Canadian Mounted Police, the Ontario Provincial Police, and the Competition Bureau of Canada. The Canadian Anti-Fraud Centre (CAFC) is the central agency in Canada that collects information and criminal intelligence on mass marketing fraud (telemarketing), advance fee fraud letters (e.g. West African), internet fraud and identity theft complaints, that have Canadian content, from North American consumers and/or victims. The CAFC does not conduct investigations, but provides valuable assistance to law enforcement agencies all over the world. The CAFC plays a key role in educating the public about specific fraudulent schemes and in the collection and dissemination of victim information, statistics and documentation, in order to provide investigative assistance to all law enforcement agencies. The data collected and analysed at the CAFC serves as a valuable tool in evaluating the effects of various types of fraud on the public. It also helps to prevent future similar crimes from taking place. The CAFC also operates the SeniorBusters program, presently consisting of more than 60 volunteer senior adults who help combat mass marketing fraud practices against seniors. The SeniorBusters program offers education, counselling and referrals to senior victims of illegal mass marketing fraud and identity theft/fraud. The Canadian Anti-Fraud Centre provides a national integrated environment that facilitates the coordination, collaboration and education of strategies and practices to disrupt and dismantle serious fraud and illegal mass marketing fraud schemes involving Canadians.'
Sources:	1. <http://www.phonebusters.com/english/index.html> (accessed 23 June 2010).

Campaign 3 – Fraud Awareness for Commercial Targets (FACT)

The FACT campaign 'is an outreach and education initiative of the Competition Bureau that provides businesses and not-for-profit organizations with the facts necessary to avoid becoming victims of fraud.'

Item	Notes
Campaign Name:	FACT (Fraud Awareness for Commercial Targets)
Organisation:	Competition Bureau of Canada
Main URL:	http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02600.html
Dates:	Ongoing
Costs:	Not disclosed
Topics covered:	Fraud
Target Audience:	Businesses and Not – for Profit Organizations
Methodology:	There is no public information on the specifics of the outreach and education initiative. The website provides free information related to fraud. Topics include: – Scam techniques – What makes your organization vulnerable – Spot Phoney Emails – Read Victim Stories – Train Your Staff to Stop Fraud – Examples of Phoney Telemarketing Calls – Examples of Phoney Invoices – Building an Anti-Fraud Plan – Report a Possible Scam
Evaluation:	Not found
Sources:	1. <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02600.html> (accessed 15 June 2010).

Campaign 4 – Fraud Prevention Forum

'The Fraud Prevention Forum is a concerned group of private sector firms, consumer and volunteer groups, government agencies and law enforcement organizations, who are committed to fighting fraud aimed at consumers and businesses. Through its partners, the Forum, which is chaired by the Competition Bureau, works to prevent Canadians from becoming victims of fraud by educating them on how to 'Recognize it. Report it. Stop it. To help prevent this problem and ensure confidence in the marketplace, the Forum organizes a month–long education campaign each March to improve consumers' awareness and understanding about the dangers of fraud'.

Item	Notes
Campaign Name:	Fraud Prevention Forum
Organisation:	Competition Bureau of Canada
Main URL:	http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/03110.html
Dates:	Ongoing
Costs:	Not disclosed
Topics covered:	All areas of fraud including online fraud
Target Audience:	Consumers
Methodology:	– Fraud awareness month every March where literally hundreds of events are organized in communities across Canada (a detailed calendar of events is provided online) – Events are organized by Forum members which consists of over 100 private and public organizations – A public advertising campaign also runs in March with advertisements on television, radio, and print
Evaluation:	Not found
Additional Information:	Membership in the Forum has grown. At launch in 2004, there were 22 members. In 2010 there are over 100. There were hundreds of fraud awareness events hosted across the country during March. The calendar of events is found at http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/03197.html. The Forum's month–long campaign of public education and awareness activities during Fraud Prevention Month include: – Scam Jams, which are one–day anti–fraud events hosted by Better Business Bureaus that combine education and information about consumer protection – Public Service Announcements in French – and English – language dailies and on radio and TV stations across the country – Other fraud prevention–related activities
Sources:	1. Fraud Prevention Forum <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/03110.html> 2. Fraud Quiz <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02922.html> 3. Victims Letters <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02923.html> 4. Calendar of fraud awareness events <http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/03197.html> (accessed 20 June 2010).

Campaign 5 – Fraud Squad TV

This online television channel operated by the Canadian Better Business Bureau provides a comprehensive library of fraud topics where users are able to access video episodes produced on each of the topic. The episodes include a description of the type of fraud in question, along with real stories of fraud, where to report incidents and how best to avoid becoming a victim.

Item	Notes
Campaign Name:	FraudSquad TV
Organisation:	Canadian Better Business Bureau
Main URL:	http://fraudcast.ca/
Dates:	Ongoing
Costs:	Not disclosed
Topics covered:	Items related to fraud (Eg. Click fraud, ATM fraud, Canadian Tax Refund Email Scams, Online Gaming fraud, Wi-Fi fraud – there are over 70 topics related to fraud.
Target Audience:	Consumers and small business
Methodology:	– Online Television Content dedicated to fraud information and prevention. A short video clip airs when you go to the website explaining the purpose of FraudSquad along with video clips of current scams – Archive of TV episodes describing scams inclusive of interviews with victims and tips for prevention – Comprehensive library with over 70 related fraud topics (information on each topic in text and video clip formats)
Evaluation:	Not found
Sources:	1. <http://fraudcast.ca/index.php> (accessed 20 June 2010).

5.3. France

Campaign 1 – Surfez Intelligent – Les Indispensables (Surf Smart – The essentials)

This site is the result of the Interdepartmental Committee for the Information Society (July 2006). The prime minister at launch underlined the priority of reinforcement of authentication on the Internet to prevent fraud attempts (such as personal data theft including banking data). The Media Development branch of the Ministry of Culture is in charge of promoting authentication best practices on Internet.

Item	Notes
Campaign Name:	Surfez intelligent – Les indispensables (Surf smart – the essentials)
Organisation:	Ministère de la Culture et de la Communication – Direction générale des medias et des industries culturelles (Ministry of Culture and Communication – General Management of media and cultural industries)
Main URL:	http://surfez-intelligent.dgmic.culture.gouv.fr
Dates:	Not applicable
Costs:	Not found
Topics covered:	General advice divided into 3 categories: – Personal data protection (check the websites' URL:, choose a safe password, keep all your electronic receipt when buying something on Internet, read the terms of service) – Emails (use a spam filter, do not click on links in an email when you do not know the sender, do not open attached files when you do not know the sender, avoid sending your phone number, create different email addresses) – Personal computer (update your system regularly, keep your logins and passwords in a safe place, activate security options)
Target Audience:	General public
Methodology:	– FAQ about 3 main themes: personal data, emails and personal computer. – Files on different topics (phishing, authentication) explaining the functioning and how to prevent it. – Charter to promote identification – Advice from professionals with links to public institutions or associations helping people with their issues or rights on internet. – Quiz to check knowledge
Evaluation:	Not found
Sources:	1. <http://surfez-intelligent.dgmic.culture.gouv.fr/spip.php?article20> (accessed 20 June 2010).

Campaign 2 – Le Portail de la securite informatique (Computer Security Portal)

This site contains general advice and specific advice on a wide range of security topics, for both end users and business audiences. The information is tailored for each audience. In addition to explaining key terms such as 'phishing', best practice approaches for each topic are offered.

Item	Notes
Campaign Name:	Le portail de la sécurité informatique (Computer security portal)
Organisation:	Agence nationale de la Sécurité des Systèmes d'Information attached to the Prime Minister (National agency for security of information systems), CNIL (national agency for protection of personal data), Microsoft, April (association promoting open source softwares), Forum des droits sur internet, e-enfance (association protecting children on internet), AFA (ISP association), Groupement des cartes bancaires (credit card grouping), UTC (university of technology Compiegne), CASES (computer security portal of Luxembourg), Signal – spam (spam reporting website) and other associations protecting children or users.
Main URL:	http://www.securite-informatique.gouv.fr/
Dates:	Not applicable
Costs:	Not found
Topics covered:	Matters relating to internet security in general, including: – e-administration – Authentication – Electronic certificates – Risk management – Cryptography / encryption – Passwords – Security policy (procedures, documents…) – Secure your network (Wi-Fi) – Secure your computer – Digital signature
Target Audience:	General public and small business
Methodology:	– Autotraining programs (lessons about different topics) – Worksheets – Configuration guide (e.g.: activate the firewall or updating the antivirus)` – Guides (protecting a child on internet) – Questions / answers – Solution to protect me (recommended software) – Advice for people who travel with their computer/pda – Security alerts (e.g.: new virus, phishing alerts) – Glossary – 10 commandments of the internet security
Evaluation:	Not found
Sources:	1. Presentation <http://www.securite-informatique.gouv.fr/gp_rubrique32.html> (accessed 20 June 2010). 2. Contact us <http://www.securite-informatique.gouv.fr/gp_page_article_id_article_157.html>

Campaign 3 – Netcity (bus with video games)

The Netcity initiative is an education and training campaign geared towards Cyber-Security issues for 9 – 12 year old students. Netcity is a bus that tours from school to school in Switzerland and nearby.

Item	Notes
Campaign Name:	Netcity.org
Organisation:	Foundation suisse pour la protection de l'enfant and Action Innocence (both in Switzerland)
Main URL:	http://www.campagne-netcity.org
Dates:	Not available
Cost	Not found
Topics covered:	– Protection of personal information – Safety tips for webcam use – Harassment, bullying, and sexual solicitation – Inappropriate online content
Target Audience:	Students aged 9 – 12 in schools
Methodology:	– Netcity.org is a physical bus that goes from school to school offering tailored Cyber-Security information for kids (the service is available for schools outside of Switzerland as well) – The bus has trained IS professionals with teaching experience who provide a Cyber-Security curriculum to students – The kids play video games teaching them about Cyber-Security and are awarded certificates after successful completion
Evaluation:	Not found
Additional Information:	Netcity is a physical bus that tours from school-to-school in Switzerland (and appears to also travel to neighbouring schools in countries just outside of Switzerland if requested), staffed by information security professionals with training in teaching. They deliver a hand-tailored Cyber-Security curriculum to the students in the form of instruction and video games. The video games in question are meant to educate students on how to surf the Internet safely. Part of the education package includes specific information and games about the protection of personal information.
Sources:	1. <www.campagne-netcity.org> (accessed 20 June 2010).

Campaign 4 – National Agency for Security of Information Systems

A set of training resources and programs offered as part of an agency site.

Item	Notes
Campaign Name:	ANSSI
Organisation:	ANSSI (National Agency for Security of Information Systems)
Main URL:	http://www.ssi.gouv.fr/
Dates:	Several formations proposed with different dates. See agenda: http://www.ssi.gouv.fr/site_article71.html
Costs:	Undisclosed
Topics covered:	Choice of training including: – Sensitization to internet security – Computer security – Wireless network security – Internet and security – Electronic certificates
Target Audience:	Generally for employees or public agents – Company directors – Security managers – Public agents – Computer specialists
Methodology:	Training courses (between 1 day and 4 weeks depending on the topic)
Evaluation:	Not found
Sources:	1. Agenda <http://www.ssi.gouv.fr/site_article71.html> (accessed 20 June 2010).

Campaign 5 – National Commission for Computer and Freedom

Commission Nationale Informatique et Libertés is an independent administrative authority promoting respect for privacy and freedom on the Internet.

Item	Notes
Campaign Name:	CNIL
Organisation:	CNIL – Commission Nationale Informatique et Libertés (National commission for Computer and Freedom) It is an administrative independent authority that controls the respect of privacy and freedom on internet.
Main URL:	http://www.cnil.fr
Dates:	Not available
Costs:	Not available
Topics covered:	Topics related to fraud: – Spam – Phishing – Personal data – Passwords – Secure local networks (Wi-Fi)
Target Audience:	General public and companies
Methodology:	– Working sheets – Guides – Legal information by phone – The institution has facebook, twitter and dailymotion pages. Videos explaining the risks of giving personal information on internet for example can be found on the dailymotion page.
Evaluation:	Not found
Sources:	1. La CNIL (composition, formation, aims) <http://www.cnil.fr/la-cnil/> (accessed 20 June 2010). 2. Also see a Who Are We Synopsis at <http://www.cnil.fr/la-cnil/qui-sommes-nous/>.

Campaign 6 – Internet Signalement

This site is an alert service to report Internet fraud, with some education sheets available.

Item	Notes
Campaign Name:	Internet – signalement
Organisation:	Ministère de l'Intérieur, de l'Outre-Mer et des Collectivités Territoriales
Main URL:	https://www.internet-signalement.gouv.fr
Dates:	Not applicable
Costs:	Not applicable
Topics covered:	This website is an alert service to report Internet fraud. It covers: – Sexual attempts towards minors – Threats, violence or incitation to commit a crime – Illicit traffic (drug, weapons…) – Spam – Defamation – Fraud There are also working sheets on how to protect your computer, and how to behave on internet in general
Target Audience:	General public
Methodology:	– Complaint forms – Advices throughout working sheets
Evaluation:	Not found
Sources:	1. <http://www.internet-signalement.gouv.fr/PortailWeb/planets?Accueil!input.action>

Campaign 7 – Signal Spam

A reporting site for spam with some related information

Item	Notes
Campaign Name:	Signal Spam
Organisation:	Association Signal – spam, supported by the French government (several ministries), Microsoft, AFA (French ISPs association), FEVAD (online sale companies association), La Poste (national post company), CNIL, National French Bank and other associations or groups.
Main URL:	https://www.signal-spam.fr
Dates:	Not applicable
Costs:	Not applicable
Topics covered:	Reporting Spam only
Target Audience:	General Public
Methodology:	– Forms to fill in order to report unwanted emails (spam) – They provide plug-ins for email software to prevent spam (for
Evaluation:	14 million reports by users in 2008
Sources:	1. Presentation <https://www.signal-spam.fr/presentation.php> (accessed 20 June 2010). 2. Activity report <https://www.signal-spam.fr/Rapport2008-VF.pdf> (accessed 22 June 2010).

Campaign 8 – f@mily en ligne (family online)

An television, website and ISP advertisement campaign carried out on multiple platforms.

Item	Notes
Campaign Name:	f@mily en ligne: Sur internet, la securité ça commence aussi pour vous (Family Online: Internet Security Begins with You)
Organisation:	French Ministry of the Family, all French ISPs, and numerous private organisations and civil society.
Main URL:	http://www.enisa.europa.eu/act/ar/deliverables/2007/loc=gov/en
Dates:	2006
Costs:	One million Euros
Topics covered:	– Personal and Banking Data Protection – Safe Blogging – Undesirable Websites – Undesirable Mail – Blocking Undesirable Materials – Parental Monitoring the Dependence of Online Games – Instant Messaging – Buying Online
Target Audience:	General Public, children against 11 – 17, and parents of children
Methodology:	– Formal advertising campaign run over two weeks over major French television stations at peak Audience: viewing time – 10 commercials targeted at different Audiences – Website logo linked to hundreds or private organisations and civil society websites – All ISPs initiated a information campaign at the same time with interactive skill set initiatives – Commercials available on YouTube as well
Evaluation:	Formal independent evaluations of project before and after. [Refer to *Section 3.2 – Campaign A. F@milie en ligne: Sur internet, la securité ça commence aussi par vous (Family Online: Internet Security Begins With You)* at page 14.]
Sources:	1. ENISA (The European Network of Information Security Agency) report on 'Information Security Awareness: Local Government and Internet Service Providers' (2007) <http://www.enisa.europa.eu/act/ar/deliverables/2007/loc=gov/en>

5.4. Germany

Campaign 1 – BSI (German Federal Office of Information Technology Security)

Government site offering counselling training, and brochure related material on cybersafety

Item	Notes
Campaign Name:	Bundesamt für Sicherheit in der Informationstechnik (BSI) – This is the German Federal Office of Information Technology Security
Organisation:	Bundesamt für Sicherheit in der Informationstechnik. BSI cooperates with the Federal Office of the Interior, especially with Bakoev, the Federal agency for public administration
Main URL:	https://www.bsi.bund.de
Dates:	01/Jan/1999 – ongoing (since 1980s preparations for the BSI)
Costs:	45,215 € in 2004 52,617 € in 2005 60,045 € in 2006 64,161 € in 2007
Topics covered:	The BSI covers a lot of different topics dealing with Cyber-Security In the field of cyber counselling the BSI is providing workshops (especially dealing with IT security)
Target Audience:	– Employees from the government – Public Audiences
Methodology:	– Publishes brochures dealing with many Cyber-Security issues – Workshops (especially in cooperation with Bakoev)
Evaluation:	Not published
Sources:	1. *Annual Report* 2006 – 2007 <https://www.bsi.bund.de/cae/servlet/contentblob/487524/publicationFile/30755/bsi_jahresbericht_2006-2007_pdf> (accessed 10 June 2010). 2. Statement about IT – security in Germany in 2007 <https://www.bsi.bund.de/cae/servlet/contentblob/479286/publicationFile/30726/lagebericht2007_pdf> (accessed 10 June 2010)

Campaign 2 – Klicksafe

The campaign wants to show the different dangers and risks of surfing the Internet and helps the public to protect themselves from cybercrimes by teaching them to understand the risks and issues.

Item	Notes
Campaign Name:	*Klicksafe*
Organisation:	This is a program founded by the EU Commission. In Germany the EU program 'Safer Internet Program' is implemented by 'Safer internet DE' alliance. The campaign should sensitise people and media to exposure to risks on the internet.
Main URL:	https://www.klicksafe.de
Dates:	2004 – ongoing (at the moment for the duration of 4 more years)
Costs:	Not available (co-funded by the EU)
Topics covered:	– Data protection – Cyber communication (chat, e-mail, spam, social networking, bullying) – Computer games and addiction – Pornography – Right – wing extremism – Depiction of violence – Exposure of eating disorders – Fraud – Peer-to-peer issues
Target Audience:	– Parents – Teachers and pedagogues
Methodology:	– Information about Internet safety topics – Free brochures and materials for the public and especially for teachers to use in school – Public commercials: 'Klicksafe spots' – Annual 'Safer Internet Day' (different events and lectures) – Hotlines and Helplines
Evaluation:	The results of the campaign are not published
Sources:	1. Homepage: <https://www.klicksafe.de> (all accessed 9 June 2010) 2. Summary of the campaign: <https://www.klicksafe.de/ueber-klicksafe/die-initiative/projektinfo/wer-ist-klicksafe.html> 3. Klicksafe spots: – 'Wo lebst Du' (= Where do you live?): <https://www.klicksafe.de/cms/ueber-klicksafe/downloads/klicksafe-werbespots/download_wo-lebst-du.html> available in English – 'Wo ist Klaus?' (= Where is Klaus?): <https://www.klicksafe.de/cms/ueber-klicksafe/downloads/klicksafe-werbespots/download_wo-ist-klaus.html>

Campaign 3 – polizei – beratung.de

Polizei – beratung.de is a campaign page by the German Police (Federal and State) for crime prevention, to warn and protect the public about many kinds of crimes and cybercrimes in particular. The aim is to raise awareness of safe Internet practices.

Item	Notes
Campaign Name:	Polizei – beratung.de
Organisation:	German Police
Main URL:	http://www.polizei-beratung.de/vorbeugung/gefahren_im_Internet/
Dates:	Not published (ongoing)
Costs:	Not available
Topics covered:	– E-Commerce – Phishing – Virus and Trojans – Risks of freeware, downloading – Fraud
Target Audience:	Everybody (Adults, Children, Elderly)
Methodology:	– Free newsletter – Brochures – 'Security compass' to check the safety of the hard – and software used – Availability of an 'Internet driver's licence'
Evaluation:	Not found
Sources:	1. Main URL: http://www.polizei-beratung.de (accessed 9 June 2010), but only this covers cybercrimes: http://www.polizei-beratung.de/vorbeugung/gefahren_im_Internet (accessed 9 June 2010). 2. Generally, in Germany the amount of all crimes is published in the annual 'Polizeiliche Kriminalstatistik' (PKS). Available at: http://www.bka.de/pks (accessed 9 June 2010). For the year 2009 the statistic (PKS) mentions 74 911 cybercrime-related cases in Germany with 37.5 percent of cases solved, see: http://www.bka.de/pks/pks2009/download/pks2009_imk_kurzbericht.pdf, p. 4 (accessed 9 June 2010).

Campaign 4 – Verbraucher – sicher – online

This is a campaign by the Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (Federal Agency for Food, Agriculture and Consumer Protection) and the Technischen Universität of Berlin (University)

Item	Notes
Campaign Name:	Verbraucher – sicher – online
Organisation:	Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz – Helps to protect consumers from cybercrimes
Main URL:	http://www.verbraucher-sicher-online.de
Dates:	Not applicable
Costs:	Not applicable
Topics covered:	– Social networks – Online banking (fraud, phishing) – Data security – Passwords – Children security – Online shopping
Target Audience:	Consumer (children, youth, parents, adults, teacher)
Methodology:	– Counsel – Online bulletin board
Evaluation:	Not found
Sources:	1. <http://www.verbraucher-sicher-online.de> (accessed 8 June 2010).

Campaign 5 – Internet surfers have rights (Federal Association of Consumer Rights)

Surfer haben Rechte ('Internet surfer have rights') is a campaign of the project 'Verbraucherrechte in der digitalen Welt' ('consumer rights in the digital world'). The organisation was founded by the Federal Association of Consumer Rights and aims to explain the digital world to consumers and enlighten them about risks and dangers of the Internet.

Item	Notes
Campaign Name:	Surfer haben Rechte (Internet surfer have rights)
Organisation:	Verbraucherzentrale Bundesverband (Federal Association of Consumer Rights)
Main URL:	http://www.surfer-haben-rechte.de
Dates:	01.01.2009 – ongoing (at least until the end of the year 2010) Term of 2 years is planned
Costs:	Not found
Topics covered:	Generally, raising awareness of safe Internet practices: – Social networking / cyberbullying – Search engines – Email provider – Online computer games – Peer-to-peer provider – Online auctions – Online shopping – Online dating agencies – Law issues: data protection, protection of young people, copyright, contract law
Target Audience:	Consumers
Methodology:	– Newsletter 'What happens in the digital world?' – Legal advice (online) – Also made available through Twitter: https://twitter.com/surferrechte – Checklists and letter templates (about different topics): http://www.surfer-haben-rechte.de/cps/rde/xchg/ls_digitalerechte/hs.xsl/768.htm
Evaluation:	Not published
Sources:	1. <http://www.surfer-haben-rechte.de/cps/rde/xchg/ls_digitalerechte/> This campaign is state-aided by the Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (Federal Agency for Food, Agriculture and Consumer Protection) because of an enactment of the Deutscher Bundestag (= German Federal Parliament). It co-operates with the campaign 'Verbraucher sicher online' 2. Available through Twitter: <https://twitter.com/surferrechte> (accessed 10 June 2010) 3. Checklists and letter templates (pdf) available at: <http://www.surfer-haben-rechte.de/cps/rde/xchg/ls_digitalerechte/hs.xsl/768.htm> (accessed 10 June 2010)

Campaign 6 – Watch your web

The *Watch your web* campaign is on behalf of the German Federal Ministry of Family Affairs, Senior Citizens, Women and Youth and the European Commission. The campaign aims to strengthen the awareness of young people to use the Internet in a free and secure way.

Item	Notes
Campaign Name:	Watch your web
Organisation:	Jugend online von IJAB – Fachstelle für internationale Jugendarbeit der Bundesrepublik Deutschland e.V
Main URL:	http://www.watchyourweb.de/
Dates:	Not found
Costs:	Not found
Topics covered:	– All topics related to young persons, especially the dangers with becoming members of social network homepages (Facebook, StudiVZ, SchülerVZ, myspace, lokalisten, wer – kennt – wen etc). – The youth should be informed about the risks of surfing the Internet – Data security
Target Audience:	Youth
Methodology:	– Video clips: <http://www.watchyourweb.de/m609386015_450.html> – Web test: which type of Internet user are you? <http://www.watchyourweb.de/m1562279832_451.html> – different events for youth – also available through Twitter: <http://twitter.com/watchyourweb> – online tutorials
Evaluation:	Not published
Sources:	1. <http://www.watchyourweb.de> (accessed 10 June 2010).

5.5. Hong Kong

Campaign 1 – INFOSEC – Information Security is Everybody's Business

This site was created in response to Internet abuse by criminals. The mission of Information Security (InfoSec) is 'to serve as an one-stop portal for the general public to effectively access information and resources on information security as well as measures and best practices for prevention of cyber crimes.'

Item	Notes
Campaign Name:	INFOSEC – Information Security is Everybody's Business – multiple, coordinated campaigns
Organisation:	InfoSec
Main URL:	http://www.infosec.gov.hk/english/sme/sme.html
Dates:	Copyright 2009; Updated June 2010
Costs:	Not Disclosed
Topics covered:	– News and Events (News and Newsletters, event calendar) – Promotion & Public Education (Promotion campaign, publications, audio visual productions, games) -information Security (what is information security?, Why does information security concern me? Why does information security concern my company?, information security in electronic services) – Virus and malicious codes (viruses & malicious codes alerts, general information, types of viruses & malicious codes outbreak, anti-virus software & malicious code detection tools) – Protecting yourself (acceptable use of the Internet, keeping self awareness for information security, handling user accounts & passwords, handling your personal information, protecting mobile devices, using instant messaging safely, using webmail wisely, using software, use public computers carefully, safe online social networking, surfing the web and e-shopping, security incident handling for individuals, protecting against spam emails, protecting against phishing attacks, protecting against malicious codes, protecting against spyware and adware, blog safely, securing your wireless network) – Protect your computer (do not let thieves steal your notebook, sharing of a home computer/notebook, protecting mobile devices, three smart tips to clean PC, using software, handling emails, securing your warless network, disposal of computer equipment containing sensitive information, secure your new PC, encrypt your data) – Protecting your business (security management, business continuity planning, backup recovery, security incident handling for companies, other tups) – Computer Related Crime (what is computer related crime?, impacts, preventative measures against computer related crimes, statistics) – Anti-Phishing (recent phishing attacks, phishing concepts and techniques, protecting against phishing attacks, FAQ's) – Technical references (Articles, guidelines and standards, security certifications, security associations and groups) – Related ordinances – Public services – Useful resources (download, useful links, quiz) – Glossary – FAQ – General users (use anti-virus and anti-malicious software, get a firewall, patching your operation system, make regular backups, secure wireless network, safe online social networking, data security when browsing the Internet, protect your privacy, protect against spam emails, protect against spyware &adware, safe e-banking and e-shopping) – Youngsters and students (One minute test, avoid fake websites, avoid phone fraud, avoid identity theft, blog safely, cyber – bullying, getting rid of viruses and malicious code, playing online games safely, protect your privacy, downloading software, use online auctions safely protect your privacy, use strong passwords, FAQ's, other resources) – Parents and Teachers (Internet content filtering, protect children from online threats, set ground rules for children, share home computer, use strong passwords, resources for parents, resources for teachers, other resources) – IT Professionals (security management, security verifications, web application security, wireless network security, patch management solution, information security standards, public key infrastructure)

Item	Notes
	– SME (control access to critical information, seek advice & support, handling security incidents, make regular backups, prevent data theft, protect computer assets, protect your website, strengthen physical security, educate & train staff, plan for information security)
Target Audience:	– Children and Youngsters – Parents and Teachers – IT Professionals – SME
Methodology:	Video, TV, audio, e.g. <http://www.infosec.gov.hk/english/promotion/audio.html> Lots of FAQs, e.g. Youngsters & Students FAQs
Evaluation:	Not found
Sources:	1. 'About Us' *InfoSec* <http://www.infosec.gov.hk/english/aboutus/aboutus.html> (accessed 23 June 2010). 2. 'Site Map' InfoSec <http://www.infosec.gov.hk/english/sitemap/sitemap.html> (accessed 23 June 2010). 3. 'Video, Games, Audio' *InfoSec* <http://www.infosec.gov.hk/english/promotion/audio.html> (accessed 23 June 2010).

Campaign 2 – Hong Kong Clean PC Day – OGCIO, HK CERT and Hong Kong Police

This government initiative, an education effort for the general public on information security awareness, has a promotion campaign pursuing a different theme each year.

Item	Notes
Campaign Name:	Hong Kong Clean PC Day
Organisation:	InfoSec
Main URL:	http://www.infosec.gov.hk/english/promotion/campaign.html
Dates:	Began on 25 November 2005 – Last PC Clean Day was in November 2009
Costs:	– Not disclosed
Topics covered:	– Security of online Transaction (2009) – Information Security for the Youth (2008) – Security Management for Businesses (2007) – Basic Personal Computer Safety for the Public (2006) General Topics – Anti-Virus Software – Personal Firewall – Security patches
Target Audience:	– Consumers
Methodology:	– Computer games (2005, 2006) – Teaching material (2005, 2006) – IT security seminars (2005, 2006, 2007, 2008, 2009) – Leaflet (2005, 2006, 2007) – Flash movies (2005, 2006) – TV programmes (2005, 2006, 2007) – Exhibition (2005, 2006) – Radio programmes on how to clean your PC (2005, 2006, 2007) – Other promotional events (2005, 2006) – Three Smart Tips Health Check (Small quiz) (2006) – Clean PC Day Carnival (2006) – Information Security Guide for Small Businesses (2007) – 5 Steps to clean your PC (2008) – Ceremony (2008) – School Visit Programme (2008, 2009) – Publications and Media Programmes (2008, 2009) – InfoSec Tours (2009) – Online Writing Competition (2009)
Evaluation:	Not found

Item	Notes
Additional Information:	2005: 'To further our education effort to the general public on information security, an information security awareness promotion campaign, 'Three Smart Tips to Clean PC' campaign, is jointly organised by the Office of the Government Chief Information Officer (OGCIO), Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Hong Kong Police Force (HKPF). In order to help the general public build up the habit of regularly cleaning up their PCs and minimise the risk of being attacked by computer virus or hackers, we have organised a 'Hong Kong Clean PC Day' on 25 November 2005, the public are invited to participate in this event by simply cleaning their PC with the following three smart tips: Scan with anti-virus software, Protect with personal firewall, Apply security patches regularly' 2006: 'Three Smart Tips' 'Information security awareness promotion is an ongoing process. To ride on the success of the 'Three Smart Tips to Clean PC' Campaign which was held last November, a second tide of the promotion campaign namely 'Hong Kong Clean PC Day 2006' is jointly organised by the Office of the Government Chief Information Officer (OGCIO), Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Hong Kong Police Force (HKPF) this November to achieve the broadest penetration of these 'Three Smart Tips' and provide the public the techniques to protect their PC from cyber attack.' 2007: 'Hong Kong Clean PC Day 2007' for SMEs 'As at December 2006, there were about 276,000 Small and medium enterprises (SMEs) in Hong Kong. They accounted for over 98% of the total business units and provided job opportunities to over 1.19 million persons, about 50% of total employment (excluding civil service), a thriving SME sector is thus vital to the economic growth of Hong Kong. With this in view, the Office of the Government Chief Information Officer (OGCIO) has teamed up again with the Hong Kong Police Force (HKPF) and Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) to jointly organise a promotion campaign namely 'Hong Kong Clean PC Day 2007'. SMEs will be the main targets of our campaign this year. We hope through our publicity programmes, SMEs can understand more about how important that information security management is to their business and hence they can assimilate the knowledge to reduce the chance of being attacked. Information security management involves a combination of prevention, detection and reaction processes. It is a cycle of iterative activities and processes that require ongoing monitoring and control. To make it easier for the public to understand the concept of information security management and take forward implementation plans, we have summarised the concepts as the following diagram and named it as 'Information Security Management Quartet'. 2008: 'Youth' 'According to a survey conducted by the Census and Statistics Department in 2007, youngsters aged from 10 to 24 had the highest rate of having used Internet services. More than 98.5 percents of them were computer and/or Internet users. The youngsters are using the Internet services mainly for communication with others, searching for / downloading information online or for offline digital entertainment. Surfing the Internet and use of computer have integrated with their daily life. Office of the Government Chief Information Officer (OGCIO), Hong Kong Police Force (HKPF) and Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) continue to co-organise the information security promotion campaign. This year, we target the 'Youth' as our main audience. We hope to enhance the understanding of youngsters of information security related topics and help them develop a proper attitude in using Internet so as to prevent themselves from becoming victims of cyber attacks.' 2009: 'Security of Online Transaction' and e-commerce 'Technology crime is on the rising trend. According to figures of Hong Kong Police Force (HKPF), the numbers of cases have been raised for about 25% to 791 in the year 2008. The latest figure in the first quarter of 2009 has reached 240, of which over half of the victims suffered financial losses. The proliferation of technology crime cases with financial loss is probably due to the recent popularity of Internet based electronic transactions such as e-auction, e-banking and e-shopping. While Internet provides a convenient and efficient channel to conduct business transaction and electronic payment, people are at the risk of financial loss due to some traps and vulnerabilities not present in the traditional pre-Internet era. Internet users have to take sufficient security considerations and precaution measures in order to minimise the risks against technology crime. The Office of the Government Chief Information Officer (OGCIO), HKPF and Hong Kong Computer Emergency Response Team Coordination Centre

Item	Notes
	(HKCERT) have continued to co-organise information security campaign. It aims to make citizens aware of the potential risks when conducting online transactions, and provides them with the proper precautions when using Internet services. This year, our main theme is 'Security of Online Transaction'. We target to enhance the understanding of information security by the Internet users, and help them to prevent the financial loss as victims of cybercrime.'
Sources:	1. 'Promotion and Public Education' *InfoSec* <http://www.infosec.gov.hk/english/promotion/campaign.html> (accessed 23 June 2010). 2. 'Three Smart Tips to Clean Your PC' Promotion Campaign (Nov 2005)' *InfoSec.* 3. 'Hong Kong Clean PC Day 2006' Promotion Campaign (Nov 2006)' *InfoSec* 4. 'Hong Kong Clean PC Day 2007' Promotion Campaign (Jun to Nov 2007)' *InfoSec* 5. 'Hong Kong Clean PC Day 2006—GenerationS' Promotion Campaign (Jan to Nov 2008)' *InfoSec* 6. 'Hong Kong Clean PC Day 2009—Security of Online Transaction' Promotion Campaign (Jan to Nov 2009)' *InfoSec*

5.6. Ireland

Campaign 1 – Research Information Technologies – Centre for Secure Information Technologies (CSIT)

The Centre is primarily a research and development site with education resources. It will bring together research specialists in complementary fields such as data encryption, network security systems, wireless enabled security systems and intelligent surveillance technology. CSIT will develop secure solutions to a number of particularly modern problems including the protection of mobile phone networks, guaranteeing privacy over unsecure networks for connected healthcare and the creation of secure 'corridors' for the seamless and rapid transit of people, thus getting around the need for conventional security at airports. Researchers will also explore the development of powerful computer processors, capable of detecting and filtering viruses and worms to protect mass information databases like financial records from malicious attack and to facilitate high definition video streaming services.'

Item	Notes
Campaign name	Research Information Technologies
Organisation:	The Institute of Electronics, Communications and Information Technology
Main URL:	http://www.ecit.qub.ac.uk/csit/
Dates:	2009 – Present
Costs:	£30M for 5 years
Topics covered:	– How businesses can work with the Institute of Electronics, Communications and Information Technology – Research (High Frequency Electronics, System – On – Chip, Digital Communications, Speech & Vision Systems) – Missions, Objectives and Values (Stimulate world-leading research and innovation, provide a balance for strategic/industrial related research, create opportunities for commercial exploitation of IPR, hout – house spin-in and spin-out start-up companies, develop a new generation of high technology engineers and entrepreneurs) – Values (People, culture, innovation, world-leading development, customer focused)
Target Audience:	– Businesses – Information Technology Scholars
Methodology:	– Online Literature – Hosts symposiums and forums for information technology scholars – Offers businesses opportunities to benefit from the Institute
Evaluation:	Not found
Additional Information:	The Centre for Secure Information Technologies (CSIT) is a new innovation and knowledge centre and is based at Queen's University of Belfast's, Institute of Electronics, Communications and Information Technology (ECIT) in the Northern Ireland Science Park, Belfast. With the total funding in the region of £30M over five years and opening in early 2009, CSIT will create the security infrastructure needed to safeguard the trustworthiness of information stored electronically, both at home and in the workplace.
Sources:	1. 'Home' *Centre for Security Information Technologies* <http://www.ecit.qub.ac.uk/csit/> (accessed 18 June 2010).

Campaign 2 – Crime Prevention: Personal Safety

This site provides straightforward information; basic questions are answered on each page, and links for further information is available. However, the site does not offer interactive games, nor a mission statement germane to Internet activities.

Item	Notes
Campaign name	Crime Prevention: Personal Safety
Organisation:	Police Service of Northern Ireland
Main URL:	http://www.psni.police.uk/index/crime-prevention/personal.htm
Dates:	Not mentioned
Costs:	Government funding
Topics covered:	– Personal Safety – Home safety – Identity Theft (Stay Safe Online, Shrug Off Shoulder Surfers, Fraud, Personal Fraud, Business Fraud, Internet/mail, identity theft/fraud, boiler rooms, high yield investments) – Scams (Link to Office of Fair Trading) - Internet Safety (Advice for Parents, links for more information) – Mobile Phone (Remember to…, if your mobile is lost or stolen) – Vehicle Safety – Buying a Car – Carers and Care Professionals
Target Audience:	– Consumers
Methodology:	– Offers links for further information – Online Literature
Evaluation:	Not found
Sources:	1. 'Crime Prevention' *Police of Northern Ireland* <http://www.psni.police.uk/index/crime-prevention/personal.htm> (all accessed 18 June 2010). 2. 'Personal Safety' *Police of Northern Ireland* <http://www.psni.police.uk/index/crime-prevention/personal/personal-safety.htm> 3. 'Identity Theft' *Police of Northern Ireland* <http://www.psni.police.uk/index/crime-prevention/personal/identity-theft.htm> 4. 'Scams' *Police of Northern Ireland* <http://www.psni.police.uk/index/crime-prevention/personal/scams.htm> 5. 'Mobile Phone' *Police of Northern Ireland* <http://www.psni.police.uk/index/crime-prevention/personal/mobile-phone.htm> 6. 'Buying a Car' *Police of Northern* Ireland <http://www.psni.police.uk/index/crime-prevention/personal/buying-a-car.htm> 7. 'Carers and Care Professionals' *Police of Northern Ireland* <http://www.psni.police.uk/index/crime-prevention/personal/carers_and_care_professionals.htm>

Campaign 3 – MakeITsecure

This is a combination project which provides a comprehensive website along with a television advertisement campaign.

Item	Notes
Campaign name	MakeITsecure
Organisation:	
Main URL:	http://www.makeitsecure.org
Dates:	2005/2006 with a new campaign in 2007 and on going
Costs:	Government funding
Topics covered:	– Phishing – Identity Theft – Spyware – Child Safety Online
Target Audience:	Consumers and children
Methodology:	– Offers links for further information – Online Literature – Television advertisement campaign
Evaluation:	Surveys pre and post campaign [Refer to *Section 3.2 – Campaign B. An evaluation of the MakeITsecure campaign* at page 15]
Sources:	1. <www.makeitsecure.org> 2. ENISA (The European Network of Information Security Agency) report on 'Information Security Awareness: Local Government and Internet Service Providers' (2007) <http://www.enisa.europa.eu/act/ar/deliverables/2007/loc=gov/en>

5.7. Japan

Campaign 1 – Secure Japan 2009: 'All Entities Should Assume They May be Subject to Accidents' – NISC (National Information Security Centre)

The main thrust of this government site is that accidents should be 'assumed', that is, breaches in security are unavoidable, and hence more emphasis should be put on response to these crises as well as on preventative measures. It contains material for many audiences including large and small business.

Item	Notes
Campaign Name:	Secure Japan 2009 – 'All Entities Should Assume They May be Subject to Accidents'
Organisation:	National Information Security Centre
Main URL:	http://www.nisc.go.jp/eng/
Dates:	2009 – 2011
Costs:	Not available
Topics covered:	– Fostering awareness of online society – Safe encryption – Utilisation of safe and reliable IT products – Information Security governance – Anti-spam measures – Malicious websites – Avoiding malware
Target Audience:	– Government Agencies and Local Governments – Critical Infrastructure – Enterprises – Individuals
Methodology:	– IT should be both managed and a 'safe work environment' to be encouraged – Strategies for response to disasters, rather than solely preventative measures – education cycle: 'awareness' – organisations to recognise that accidents will happen and doing review of counteractions after accidents occur 'cooperation' – organisations to look into the possibility of liaising or task sharing security measures with other organisations 'maturity' – every organisation to implement actions relevant to them as part of the 'Accidents Assumed Society' – additional PR activities linked to human resource development
Evaluation:	Not found
Additional Information:	'Secure Japan 2009' is the beginning of the Second National Strategy, and as the name suggests, has been modelled on the basis of successes and failures of the previous First National Strategy starting from 'Secure Japan 2006'. The main thrust of the new policy is that accidents should be 'assumed', that is, breaches in security are unavoidable, and hence more emphasis should be put on response to these crises as well as on preventative measures. Government agencies are to formulate their own systems and provide an 'Information Security Annual Report', including an assessment on whether the ideas they implemented were successful, to be demonstrated using 'objective indicators such as numerical representation.' For enterprises, the emphasis of the campaign is to promote information security governance as 'part of corporate governance'. There is a strong emphasis on audits of information security systems, and third party assessments of them. The campaign at individuals is targeted at all age groups, both in terms of raising awareness of problems and 'improving media literacy'. This campaign also has a small international element, in that materials have been provided in English and published online, in the hope of making this sort of strategy known both inside and outside Japan.
Sources:	1. 'Contents' *National Information Security Centre* <http://www.nisc.go.jp/eng/index.html> (accessed 24 June 2010). 2. 'Secure Japan 2009' *Information Security Policy Council* <http://www.nisc.go.jp/eng/pdf/sj2009_eng.pdf> (accessed 24 June 2010).

5.8. Korea

Campaign 1 – KISA

KISA is an amalgamation of Korea Information Security Agency, National Internet Development Agency and Korea IT International Cooperation Agency. 'Korea Internet & Security Agency will endeavour to make our country be reborn to a strongest country on Internet and a safe advanced Internet country, through promoting Internet services, protecting information over Internet, and cooperating internationally with other countries.

Item	Notes
Campaign Name:	KISA
Organisation:	Korea Information Security Agency (KISA).
Main URL:	http://www.kisa.or.kr/eng/index.jsp
Dates:	2009 till the present
Costs:	Not available
Topics covered:	– Hacking, such as the DDoS (Distribute Denial of Service) – Identity theft
Target Audience:	Community generally
Methodology:	– personal information infringement and illegal SPAM call centres – future Internet outlook, economical analysis, and threat forecasting – technology support and establishment of security measures
Evaluation:	Not found
Additional Information:	In addition, another website launched by KISA <http://www.boho.or.kr> is a portal site that provides businesses with the means to conduct security self – assessments.
Sources:	1. 'Main Activities' *Korea Information Security Agency* <http://www.kisa.or.kr/eng/pages/main/main.jsp> (accessed 24 June 2010). 2. 'About KISA' *Korean Information Security Agency* <http://www.kisa.or.kr/eng/pages/about/about_chairman.jsp> (accessed 24 June 2010).

5.9. New Zealand

Campaign 1 – NetSafe Netbasics

Netbasics is one of several campaigns created by the Netsafe Group intended to educate and support various groups in relation to cybersafety issues. Net safe's Strategic Partners include the Ministry of Education, and InternetNZ. The various members of the Netsafe Group represent different perspectives from across New Zealand's cyberspace community, from areas including: government, education, law, industry, community, parents and caregivers and young people.

Item	Notes
Campaign name	Netsafe Netbasics
Organisation:	Netsafe Group
Main URL:	http://www.netsafe.org.nz/
Dates:	1998 till present
Costs:	Not available
Topics covered:	– Dangerous downloads – Firewall protection – Phasing and fake websites – Password Protection – Staying safe online – Updating for security – Backing up important data
Target Audience:	Home computer users (specifically families)
Methodology:	– Create animated stories to demonstrate important risks and issues in – Online guidelines provided alongside each 'episode' to assist users manage the risks identified
Evaluation:	Not found
Additional Information:	In 2008, the Netbasics web site was awarded the gold medal in the Interactive Media and Web Design category of the Design Institute of New Zealand's Best Design Awards.
Sources:	1. 'Home' *Netsafe* <http://www.netsafe.org.nz/index.php> (accessed 23 June 2010). 2. 'Welcome to Netbasics' *Netsafe Netbasics* <http://www.netbasics.org.nz/> (accessed 23 June 2010).

Campaign 2 – Hector's World

Hector's World Limited is a subsidiary of Netsafe. In the wake of previous successes in New Zealand, since 2008, Hector's World has begun to foster international partnerships, in both the UK and in Australia through the Australian Communications and Media Authority (ACMA).

Item	Notes
Campaign name	Hector's World
Organisation:	Netsafe
Main URL:	http://www.hectorsworld.com/island/index.html
Dates:	2003 - present
Costs:	Not available.
Topics covered:	General topic area of 'digital citizenship', the responsibilities and benefits of belonging to the online community, specifically in the categories of: – Digital literacy – Media literacy – Online safety and security (cybersafety) – Information literacy
Target Audience:	Children 2 – 9 yrs of age, and their parents/caregivers and teachers.
Methodology:	– Provide children with intellectually and emotionally stimulating way to learn about the digital world – High quality 2D animation, games and music including: episodes, puzzles and games, MP3 music files, downloadable story books and related activities – Support documents available for parents and teachers in the form of lesson plans etc
Evaluation:	Not found
Additional Information:	The core value of Hector's World is to 'make a difference in young children's lives by offering them the skills and knowledge they need to mature into confident and capable online citizens'. In 2010, Hector's World won the inaugural Australia and New Zealand Internet Best Practice Awards for Best Security Initiative. These awards 'recognise organisations, businesses, groups and individuals that have made significant contributions towards the security, openness, diversity and accessibility of the Internet.' Although the primary success of Hector's World thus far has been through implementation in both New Zealand and Australian schools, they aim to continue to develop relationships abroad with both government and corporate partners with the intention of more widely disseminating their content.
Sources:	1. 'Information Island' *Hector's World* <http://hectorsworld.netsafe.org.nz/about-us/history-of-hectors-world/> (accessed 23 June 2010).

Campaign 3 – NetSafe: Cyberbullying

The primary focus of this section is Cyber bullying. The site provides young people, parents, and teachers basic questions and answers about Cyber bullying. In addition to the basic facts provided, there are also videos for young people, parents, and teachers to watch and share with family and friends.

Item	Notes
Campaign Name:	Cyberbullying
Organisation:	NetSafe [sic]
Main URL:	http://www.netsafe.org.nz/
Dates:	2000 – 2009
Costs:	Not mentioned
Topics covered:	For Young People – What is cyberbullying? – What does cyberbullying look like? – Is cyberbullying a big deal? – What can I do to prevent cyberbullying? – What can I do if I am being cyberbullying? – Cyber bullying at your school – Cyber bullying on your favourite sites – Cyber bullying on IM – Cyber bullying and your mobile – What can I do to help someone being cyber bullied? – Cyberbullying on websites and IM - When to call the police – What if I'm scared about getting involved? – At a Distance—standing up to cyberbullying
Topics covered:	For parents – What is cyberbullying? – What does cyberbullying look like? – Is cyberbullying a big deal? – What can I do to prevent cyberbullying – More help and advice – What can I do if a child is being cyber bullied? – Cyber bullying and school – Cyber bullying on websites – Cyber bullying on IM/online chat – Cyberbullying and mobile phones – When to call the police – At a Distance—standing up to cyberbullying – Video interviews with teachers
Topics covered:	For Teachers – What is cyberbullying? – What does cyberbullying involve? – How is cyberbullying different to other forms of bullying? – Is cyberbullying a big deal? – The effects of cyberbullying – Cyber bullying and the law – What can I do to prevent cyberbullying amongst my students? – Classroom interventions – Are 'bystanders' important? – The 4 types of bystander – How bystanders can help – What do principals and teachers say? – Video interviews – At a Distance—standing up to cyberbullying – Let's fight it together—Cyberbullying film by Childnet International

Item	Notes
Target Audience:	– Young People – Parents – Teachers
Methodology:	– Online Literature – Videos
Evaluation:	Not found
Sources:	1, 'For Young People' *Cyberbullying* <http://www.cyberbullying.org.nz/youngpeople/> (accessed 23 June 2010). 2. 'For Parents' *Cyberbullying* <http://www.cyberbullying.org.nz/parents/> (accessed 23 June 2010). 3. 'For Teachers' *Cyberbullying*<http://www.cyberbullying.org.nz/teachers/> (accessed 23 June 2010).

Campaign 4 – NetSafe: In My Day

'InMyDay' focuses on educating adults on activities young people engage in online, which for adults occurred offline. For instance, when adults were in school, talking to friends after school may have happened on campus; in contrast, children chat with friends online. 'InMyDay' is designed to help parents understand the new environment of the Internet and challenges that children may face in the cyberspace.

Item	Notes
Campaign Name:	In My Day
Organisation:	Netsafe
Main URL:	http://www.inmyday.org.nz/
Dates:	2000 – 2009
Costs:	Not Mentioned
Topics covered:	– Publishing Content Information (Unacceptable Digital Format, Copyright Infringement, Harassment/Abuse) – Online Trading Information (Scams, Computer Security) – Computer Security Information (Have you heard of a virus?, Can computers get infected?, How does a computer get infected?, What does a computer look/act like when it is infected?, What can you do if it is infected?, How can you stop a computer from getting infected?) – Communicating Information (Inappropriate/Scary Material, Scams, Time Management, Exposure to Sexual Content, Unacceptable Digital Footprint, Harassment/Abuse, Computer Security) – Some Websites allow you to do research (Computer Security, Inappropriate/Scary Material, Exposure to Sexual Content) – Official Publications (Exposure to sexual content, Copyright Infringement, Copyright Infringement, Computer Security, Time Management, Inappropriate/Scary Material)
Target Audience:	– Parents
Methodology:	– Online Literature – Video
Evaluation:	Not found
Additional Information:	'InMyDay' holds the belief that 'parents and caregivers have an opportunity to support young people as they learn to manage the challenges that cyberspace will inevitably offer up. Conversation is a powerful tool for parents and caregivers to use in supporting young people.' When adults equip themselves with the knowledge of the issues at play, they will be able to engage and support young people 'in their day'.
Sources:	1. 'In My Day' *In My Day* <http://www.inmyday.org.nz/> (accessed 23 June 2010).

Campaign 5 – Schools & ECE

This aspect of the Netsafe campaign is intended to deliver and communicate Netsafe's combined resources (including Hector's World) directly to schools. Although the Netsafe team will do staff and/or parent presentations on their material on request, they 'would rather see teachers within a school delivering all facets of cyber-citizenship education themselves'.

Item	Notes
Campaign name	Schools & ECE
Organisation:	Netsafe
Main URL:	http://www.netsafe.org.nz/
Dates:	1998 till present
Costs:	Not available
Topics covered:	– Mobile phones – Copyright – School sites – Blogs – Social Networking – Bullying and harassment – Spam
Target Audience:	Schools and Early Childhood Education facilities
Methodology:	– Netsafe Kit for Schools – 'The Grid', 'a progression of cyber-citizenship attributes, appropriate learning objectives, suggested activities and recommended resources' – 0508 NETSAFE, a 'confidential advice and referral service for schools dealing cybersafety incidents' – pamphlets and posters – other teaching resources, including staff training e-learning modules – staff and parent presentations
Evaluation:	Not found
Sources:	1. 'Netsafe Education Sector' *Netsafe* <http://www.netsafe.org.nz/keeping_safe.php?sectionID=education&pageID=63&menuID=63> (accessed 23 June 2010).

Campaign 6 – How to Prevent Identity Crime

This site provides very basic information on identity theft. It consists of only a one-page informational dialogue on identity theft, offering consumers a definition of identity theft and fraud, how to prevent identity theft, and what procedures victims of identity theft should follow.

Item	Notes
Campaign Name:	Safer Communities Together: How to Prevent Identity Crime
Organisation:	New Zealand Police
Main URL:	http://www.police.govt.nz/safety/home-identity-crime.html
Dates:	Not Mentioned
Costs:	Not Disclosed
Topics covered:	– How to prevent identity crime – Why you should protect your identity – Identity fraud – Identity theft
Target Audience:	– Consumers
Methodology:	– Online Literature – Provides links to other sites
Evaluation:	Not found
Sources:	1. 'How to Prevent Identity Crime' *New Zealand Police* <http://www.police.govt.nz/safety/home-identity-crime.html> (accessed 23 June 2010).

Campaign 7 – Child Safety Online

This site provides very basic information to educate parents on how to a safe Internet environment for their children. It consists of an informational dialogue on cyber safety in an effort to alert parents of online threats, and the benefits of the Internet. Most notably, parents are provided with a guideline on how to properly advise their children about cyber safety.

Item	Notes
Campaign Name:	Child Safety Online
Organisation:	Department of Internal Affairs
Main URL:	http://www.dia.govt.nz/diawebsite.nsf/wpg_URL:/Resource-material-information-We-Provide-Child-Safety-Online?OpenDocument&ExpandView
Dates:	Not Mentioned
Costs:	Not Disclosed
Topics covered:	– What are the risks? – Guidelines for parents – Rules for Online Safety – Online Safety Agreement – Links to more Internet Safety Information – Return to Censorship Compliance—Services – Return to Censorship Compliance—Information We Provide
Target Audience:	– Consumers
Methodology:	– Online Literature – Provides links to other sites
Evaluation:	Not found
Sources:	1. Child Safety Online *Department of Internal Affairs* <http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-information-We-Provide-Child-Safety-Online?OpenDocument&ExpandView> (accessed 23 June 2010).

Campaign 8 – CyberKidz

'The Cyberkidz website is designed to help parents and teachers educate children about safety on the Internet. There are seven 'Safety Points' illustrated through the characters 'Webstar', 'Whizkers' and 'Danger Claws'.

Item	Notes
Campaign Name:	CyberKidz
Organisation:	Elimination of Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes (ECPAT)
Main URL:	http://www.dia.govt.nz/diawebsite.nsf/wpg_URL:/Resource-material-information-We-Provide-Child-Safety-Online?OpenDocument&ExpandView
Dates:	Not Mentioned
Costs:	Not Disclosed
Topics covered:	– Fun Puzzle -invent a Land – Quiz – Teachers – Parents (The basics of online safety, such as not giving personal information to strangers)
Target Audience:	– Consumers
Methodology:	– Online Literature – Provides links to other sites
Evaluation:	Not found
Additional Information:	It is important that parents provide a supportive environment for the online explorations of their children and that they understand both positive and negative aspects of the Internet. It is recommended that parents place computer(s) in an open area where the screen can be monitored while their children are online. Using the Internet can be an important bonding time for families and we recommend that parents spend regular times exploring the Net with their children. This time may be for purposes of entertainment or school homework. This will help children to respect the Internet as a valuable resource for learning as well as for fun. The 'Teachers' section of the website gives detailed suggestions of how to use this website to teach children about safety on the Internet. We recommend that parents read through the seven safety points with their child and help them to read through the 'Quiz'. The 'Invent-a-Land' activity is designed for printing from the computer and the picture is then completed offline. Whereas, the 'Fun Puzzle' is designed for use on the computer. The 'Safe Links' section of the website provides a list of safe websites compiled by the team at Netguide Magazine. These websites have been recommended as safe for children to use.'
Sources:	1. <http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-information-We-Provide-Child-Safety-Online?OpenDocument&ExpandView> (accessed 16 June 2010).

Campaign 9 – E-Government

This government site offers literature and links about e-government.

Item	Notes
Campaign Name:	E-Government
Organisation:	E-Government
Main URL:	http://www.e.govt.nz/
Dates:	2001 – 2009
Costs:	Not Disclosed
Topics covered:	– About E-Govt (Programme, E-government agency checklist, FAQ's) – E-Government Strategy (Strategy update, Nov. 2006 Revised Strategy, Cabinet Paper) – Policies (Open Source, Open Source Briefing, Governance and Funding, Trusted Computing &DRM, Principles and Policies, Standards and Guidelines 2007) – Trust and Security (Trusted Computing Technologies: Briefing, Trust and Security on the Internet, Overseas hosting risk Analysis, Government Use of Offshore Information and Communications Technology, Service Providers) – IP Rights (definitions, Purpose of the Guidelines, Scope of the Guidelines, Overview of the Guidelines, Background to the Guidelines, Aim Statement, Guidelines, Decision Process, Licence Agreements, Appendix One, IPR Guidelines, FAQ) - Information and Data (Promoting government information and data re-use, policy framework for government held information, exposing non – personal government data in new ways, New Zealand government open access and licensing, New Zealand government open access and licensing (NZGOAL) framework, NZGAAL submissions) – Standards (Web standards, Metadata (NZGLS), NZGLS metadata standards, Metadata management, interoperability (e-GID), eGID Version 3.3, interoperability cabinet paper, interoperability FAQ's, development of a standard, authentication standards, extensible mark-up language, extensible name and address mark-up language, data management, extensible business reporting language, governance, geospatial information standards, network time protocol, public protection and disaster relief) – Federated Enterprise Architecture (Enterprise architecture definitions, enterprise architecture framework, DEA principles, the trust principle, the sovereignty principle, the asset principle, the accessibility principle, the consistency principle, the agility principle, the user – centric principle, NZFEA framework reference models, FEA framework reference models)
Target Audience:	– Consumers
Methodology:	– Online Literature – Provides links to other sites
Evaluation:	Not found
Additional Information:	'E-government is a way of tapping unrealised potential for high quality government in New Zealand. It enables government agencies to separately and collectively lift their performance and deliver better results through using information and technology in new, more collaborative, ways. E-government delivers better results by adapting government to the environment of the information age and the Internet. The public has invested hugely in the information, technology, and processes used by government, as well as in people and public management systems. E-government makes the best of this investment to deliver improved services to New Zealanders. Technological change is only part of achieving this goal, and the Internet will not fully replace all other way government relates to people. Technology does not guarantee better public sector performance on its own. Success also depends on making ongoing improvements to the design, operation, and culture of the public sector, so that it can better respond to the changing demands of New Zealanders. E-government is best understood in the context of: the Government's broader goals to improve public management; what New Zealanders (people and business) want form e-government; public sector ethics, values and standards; and new thinking about how service delivery should be electronically enabled'.
Sources:	1. 'Home' *E-Government* http://www.e.govt.nz/ (accessed 23 June 2010). 2. 'Site Map' *E-Government* http://www.e.govt.nz/sitemap (accessed 23 June 2010). 3. 'About' *E-Government* http://www.e.govt.nz/about-egovt (accessed 23 June 2010).

5.10. Singapore

Campaign 1 – Go Safe Online (Cyber-Security Awareness Alliance)

'The Cyber-Security Awareness Alliance members aim to reach out to the public and private sectors and individuals through 'organising and sponsoring events such as seminars, talks, road shows and training workshops; creating infocomm security-related collateral for user and business groups, and making it available either online, in print or through broadcast media; and offering infocomm security advice for user and business groups, through online, print or broadcast channels.'

Item	Notes
Campaign Name:	Go Safe Online
Organisation:	Cyber-Security Awareness Alliance
Main URL:	http://www.gosafeonline.sg/
Dates:	2008 – 2010
Costs:	Not Disclosed
Topics covered:	(Broad) – How to form a positive Cyber-Security culture in Singapore – Essential infocomm security practices for private and people sectors (found on fact sheet)
Target Audience:	– Public sectors – Private sectors – People Sectors
Methodology:	– Online Literature – Organising and sponsoring seminars, talks, road shows, and training workshops – Creating infocomm security – related collateral for user and business groups, and making it available either online, in print or through broadcast media – Offering infocomm security advice for user and business groups, through online, print or broadcast channels.
Evaluation:	
Additional Information:	The Infocomm Development Authority of Singapore and partners from the public and private sectors formed a Cyber-Security Awareness Alliance (Alliance) in April 2008. The aim of the Alliance is to: – Build a positive culture of Cyber-Security in Singapore where infocomm security becomes second nature for all infocomm users; and – Promote and enhance awareness and adoption of essential infocomm security practices for the private and people sectors.
Sources:	1. 'Fact Sheet' *Cyber-Security Awareness Alliance* <http://www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20050906094800/ISS22Mar10AnnexB.pdf> (accessed 23 June 2010). 2. 'Home' *Cyber-Security Awareness Alliance* <http://www.gosafeonline.sg/> (accessed 23 June 2010).

Campaign 2 – Virtual Cyber-Security Park

In an effort to educate school children on good Cyber-Security, Singapore has opened a 'Virtual Cyber-Security Park'. This was announced in March 2010 as part of the Infocomm Security Masterplan 2 (MP2). Students attending primary school in Singapore will have the opportunity to navigate the 'Virtual Cyber-Security Park' to learn good Cyber-Security in an engaging and enjoyable way.

This is a new initiative and more information may be released soon.

Item	Notes
Campaign Name:	Virtual Cyber-Security Park
Organisation:	Infocomm Security Masterplan 2
Main URL:	(announced, but not yet implemented)
Dates:	– Not yet released (please double check)
Costs:	– Not disclosed (please double check)
Topics covered:	(Broad) – Cyber Wellness – Cyber-Security – Cyber Safety
Target Audience:	– Grade School Children
Methodology:	Modelled after the Road Safety Community Park in the East Coast which welcomes groups of students for road – safety lessons in a scaled – down road network, the Virtual Cyber-Security Park will show today's increasingly wired children how their seemingly innocuous actions on the Web can come back to haunt them. The online park will use 3 – D technology to re-create scenarios young ones encounter while online, from creating social networking profiles to playing online games.
Evaluation:	Not found
Sources:	1. Information on MP2 <http://www.ida.gov.sg/News%20and%20Events/20050906094800.aspx?getPagetype=20> (accessed 23 June 2010).

Campaign 3 – Fasten Up! (Infocomm Security Division, Singapore)

The Infocomm Security Division 'is chartered to develop and promote a secure infocomm environment for the Public, Private and People Sectors. iSec plays a leading role to establish and facilitate robust and secure government, and national infocomm infrastructures in Singapore. It oversees the establishment of infocomm security policies, standards and guidelines for the Government. In addition, iSec plans and implements central security infrastructures and services and promotes infocomm security awareness to the Public Sector.

Item	Notes
Campaign Name:	Fasten Up!
Organisation:	Infocomm Development Authority Singapore
Main URL:	http://www.singcert.org.sg/awareness/
Dates:	– Not Mentioned
Costs:	– Not Disclosed
Topics covered:	– What is a wireless network? – What are some of the dangers connected to wireless networks? – Protect yourself and your computer when using a wireless network – Firewall – Anti-Virus – Scams – Updates – Passwords – Secure Wi-Fi Surfing – Typical wireless network set-up – Major Wireless network security issues – Protect Yourself As You Surf – Secure Your Wireless Network – Steps to check which wireless network you are connected to – Steps to disable the auto – connect feature in your wireless settings – Steps to connect to your secure wireless network – Glossary
Target Audience:	– Consumers
Methodology:	– Quiz – http://www.singcert.org.sg/awareness/quiz.htm – Video – Cartoons – Online Literature
Evaluation:	Not found
Additional Information:	The Infocomm Security Division established the 'Fasten Up!' campaign. 'Beyond the Public Sector, iSec provides incident handling services through SingCERT, reviews infocomm security technologies, collaborates with the industry in infocomm security R&D and works closely with critical infrastructure owners/operators to ensure high service availability. It also promotes infocomm security awareness among the general public and industry through seminars, workshops and other outreach activities.'
Sources:	1. 'Home' *Infocomm Security Division* <http://www.singcert.org.sg/awareness/> (accessed 23 June 2010) 2. 'Wi-Fi' *Infocomm Security Division* http://www.singcert.org.sg/awareness/wirelesslan.htm (accessed 23 June 2010). 3. 'Quiz' *Infocomm Security Division* http://www.singcert.org.sg/awareness/quiz.htm (accessed 23 June 2010).

Campaign 4 – Once Upon a Cyberspace (Singapore Media Development Authority)

The Media Development Authority (MDA) is a Singaporean regulatory body for, among other things, film and broadcast classifications. They also play an active role promoting 'Cyber Wellness'. Commissioning the 'Once Upon a Cyberspace' animated series is one of the various ways in which they attempt to reach the community.

Item	Notes
Campaign Name:	Once Upon a Cyberspace
Organisation:	Singapore Government Media Development Authority
Main URL:	http://www.mda.gov.sg/Pages/Home.aspx
Dates:	April 2009
Costs:	Not available
Topics covered:	– Dangers of sharing personal information online – Game addiction – Internet viruses – Cyber bullying – Invasion of privacy
Target Audience:	Children, ages 10 – 14 years
Methodology:	– a holistic outreach approach to educate not just youth, but also educators, parents and the general public – Specifically, 'Once Upon A Cyberspace' is a '3D animated series ran as six 1 – minute interstitials on MediaCorp's okto [TV channel] channel for six running weeks'
Evaluation:	Not found
Additional Information:	'Cyber wellness refers to the positive well – being of Internet users and a healthy cyber culture for the Internet community. It involves an understanding of the risks of harmful online behaviour, an awareness of how to protect oneself and other Internet users from such behaviour, and a recognition of the power of the Internet to benefit oneself and the community at large.' The MDA 'works closely with a number of partners from the public, people and private sectors to raise awareness on the core values of cyber wellness through various activities. In particular, MDA works closely with Inter – Ministry Cyber Wellness Steering Committee (ICSC) and Internet and Media Advisory Committee (INMAC) in identifying and facilitating key cyber wellness initiatives.'
Sources:	1. 'About Cyber Wellness' *Media Development Authority* <http://www.mda.gov.sg/Public/Pages/CyberWellness.aspx> (accessed 24 June 2010).

5.11. United Kingdom

Campaign 1 – Cyber-Security Programme

This site is crafted with an edgy style in an effort to attract consumers. Information found on this site is written in common terms for non–technical users. Since the focus of the site is Identity Theft, the organization provides a number of articles, and answers basic questions, about how to prevent identity theft, and how victims can assist themselves. Users are encouraged to download posters and leaflets that can be passed out to their friends and family.

Item	Notes
Campaign Name:	Cyber-Security Programme
Organisation:	Cyber-Security Programme-Collaborates within the Digital System's Knowledge Transfer Network (1)
Main URL:	http://www.ktn.qinetiq-tim.net/about.php
Dates:	Ongoing, the establishment of the campaign is unclear
Costs:	– It is unclear what the cost is to maintain the organization. – The Programme receives various funds to sponsor competitions that promote research in specified Cyber-Security issues. (3)
Topics covered:	– Assistance for users of security technology – Facilitate promises made by Trusted Computing – Focus on 'the Financial Services sector by studying their previous experience in implementing global and cost effective solutions; seeking to transfer lessons learnt, best practice and identify identity capability and technology gaps.' – Raising awareness of safe Internet practices – 'Investigate why it is that we still develop code with potential security vulnerabilities when the theory on how develop code without such coding errors has been available to the community for many years. Then to propose an approach to enabling the software industry to produce higher integrity software.' – All from reference (3)
Target Audience:	Scholars in the field, business leaders, users of large scale identity management (Reference 2)
Methodology:	– Stimulate conversation amongst scholars and business leaders to find possible solutions, which address the organization's current priorities
Evaluation:	It may be possible to find evaluations for projects funded by this foundation
Sources:	1. Cyber-Security Programme, *Knowledge Transfer Networks,* <http://www.ktn.qinetiq-tim.net/index.php> (accessed 20 May 2010). 2. Funding Opportunities, *Knowledge Transfer Networks,* <http://www.ktn.qinetiq-tim.net/competitions.php> (accessed 20 May 2010). 3. Current Priorities, *Knowledge Transfer Networks* <http://www.ktn.qinetiq-tim.net/about.php?page=ab_priorities> (accessed 20 May 2010).

Campaign 2 – Identity Theft: Don't become a victim (CIFAS)

'CIFAS provides a range of fraud prevention services to its Members, including a fraud avoidance system used by more than 260 UK organisations across a number of business sectors, as well as by public sector bodies.'

Item	Notes
Campaign Name:	Identity Theft: Don't become a victim
Organisation:	Identity Theft UK – With: City of London Police, Royal Mail, Home Office, CIFAS, FSA, Metro Police, SOCA, DVLA, Call Credit, Experian, Equifax, National Fraud Authority, BBA, Identity and Passport Service, UK Cards Association, BSIA, FFA, BSIA (a)
Main URL:	http://www.identitytheft.org.uk/
Dates:	Ongoing (a)
Costs:	– Not mentioned
Topics covered:	– Identity Theft – How to Protect Yourself – Who can help – What can be done – Are you a victim (all above b) – For businesses, an individual must have an account to access information on website. There is training regarding identity theft through this portal. (c)
Target Audience:	– Public – Businesses (a)
Methodology:	– Online literature – Videos on website (a and b)
Evaluation:	Not found
Additional Information:	'CIFAS is a not for profit membership association representing the private and public sectors and operating in the public interest ... dedicated to identification of financial crime, and prevention of fraud and staff fraud. CIFAS' purpose is 'to protect the interest of CIFAS Members from the actions of criminals by pooling information on fraud and attempted fraud; ensure that innocent members of the public who are victims of fraud are not prejudiced by misuse of their identities and documentation; expand crime prevention data – sharing to encompass both private and public sectors in the public interest.' CIFAS' vision is to 'specialize in the field of application, identity, first party and staff fraud and position [themselves] as the first choice of organization in both the private and public sectors to share fraud data; to be the leader in providing fraud prevention services to both sectors; to continue successfully to balance the needs of the organization with the rights of individuals and to be open to public scrutiny'
Sources:	1. 'Homepage' Identity Theft <http://www.identitytheft.org.uk/> (accessed 20 May 2010) 2. 'Identity Theft: Don't Become a Victim' Identity Theft <http://www.identitytheft.org.uk/default.asp> (accessed 20 May 2010) 3. 'Identity Theft: Don't be a Victim' (Business) Identity Theft <http://www.identitytheft.org.uk/security.asp?action=in> (accessed 20 May 2010)

Campaign 3 – Credit Industry Fraud Avoidance System (CIFAS)

This industry site offers groups that subscribers can join. In these groups, participants learn about how to avoid fraud.

Item	Notes
Campaign Name:	Credit Industry Fraud Avoidance System (CIFAS)
Organisation:	CIFAS – UK's first Non-profit fraud prevention data scheme
Main URL:	http://www.cifas.org.uk/default.asp?edit_id=252-28
Dates:	– 2007 under the Serious Crime Act 2007 – Ongoing
Costs:	Not Found
Topics covered:	– Identity Fraud (Why is ID so important?, Why is ID fraud serious?, how fraudsters work, avoid being a victim) – Staff Fraud (CIFAS Staff fraud database, Joining CIFAS' Staff fraud) – Protective Registration (For individuals, for organizations)
Target Audience:	– Public – Private businesses
Methodology:	– There are groups offered through the organization subscribers can join. In these groups, participants learn about how to avoid fraud.
Evaluation:	Not found.
Sources:	1. 'Home' *CIFAS: The UK's Fraud Prevention Service* <http://www.cifas.org.uk/default.asp?edit_id=252-28> (accessed 20 May 2010). 2. 'Identity Fraud' *CIFAS: The UK's Fraud Prevention Service* <http://www.cifas.org.uk/default.asp?edit_id=252-28> (accessed 20 May 2010). 3. 'Staff Fraud' *CIFAS: The UK's Fraud Prevention Service* <http://www.cifas.org.uk/default.asp?edit_id=252-28> (accessed 20 May 2010). 4. 'Protective Registration' *CIFAS: The UK's Fraud Prevention Service* <http://www.cifas.org.uk/default.asp?edit_id=252-28> (accessed 20 May 2010).

Campaign 4 – National Identity Fraud Prevention Week

National Identity Fraud Prevention Week is a nationwide effort to help in the battle against identity fraud. This website offers a range of resources to help [civilians] and business avoid the costly and debilitating effects of this crime.

Item	Notes
Campaign Name:	National Identity Fraud Prevention Week
Organisation:	National Identity Fraud Prevention Week with Royal Mail, British retail Consortium, Fellowes, Experian, Call Credit, National Fraud Authority, Identity Passport Services, CIFAS, Equifax, Metropolitan Police, British Chambers of Commerce, FSB, ACPO (b)
Main URL:	http://www.stop-idfraud.co.uk/
Dates:	October 12th – 18th each year
Costs:	Not mentioned
Topics covered:	– What is ID Fraud – How to prevent ID fraud – The facts – How ID fraud occurs – Real life stories – Guidance for fraud victims (a)
Target Audience:	– Public – Businesses (a)
Methodology:	– Encourages participants to post the organization's emblem on MySpace, Facebook, or Twitter – Reach out to participants through online literature and videos on website
Evaluation:	Not found
Additional Information:	Identity Fraud is one of the UK's fastest growing crimes, affecting individuals and businesses alike. Although most people know about it, our research shows that consumers and businesses are not aware of, or not taking the steps they could and should be taking to fully protect themselves. National Identity Fraud Prevention Week is a nationwide effort to help in the battle against identity fraud. This website offers a range of resources to help [civilians] and business avoid the costly and debilitating effects of this crime.
Sources:	1. 'Home' http://www.stop-idfraud.co.uk/> (accessed 20 June 2010). 2. 'Partners' <http://www.stop-idfraud.co.uk/partners.aspx> (accessed 20 June 2010). 3. 'Get involved' <http://www.stop-idfraud.co.uk/show-your-support.aspx> (accessed 20 June 2010).

5.12. United States

Campaign 1 – National Cyber-Security Alliance (2001)

The primary aim of the National Cyber-Security Alliance is to raise awareness of cyber threats towards children, parents, teachers, college students, and small businesses. The organization's site provides the public with online resources to defend themselves against online threats, such as phishing, spam, and scams, as well as information that assists parents with educating their children about online threats.

Item	Notes
Campaign Name:	National Cyber-Security Alliance-Helps drive 'National Cyber-Security Awareness Month' in addition to other responsibilities (1)
Organisation:	National Cyber-Security Alliance
Main URL:	http://www.staysafeonline.org/ (1)
Dates:	2001 – ongoing (1) – No longer receiving funds from Homeland Security, but it still associated with that government department (2)
Costs:	From the government: $1,000,000 in 2006 $1,250,000 in 2007 $1,500,000 in 2008 – Funds were received in 2009, but it is not stated how much money was provided the organization. – The amounts listed do not include money received from private corporations (2)
Topics covered:	– Personal computer protection through three core safety techniques: Installation of an anti-spyware program, installation of an anti-virus program, installation of a firewall program – Protecting material on computer through backing up data – Protection of Internet practices through type of Internet connection – Protect Children: Filtering, and cyber bullying – Protect yourself against e-mail phishing and spam, online shopping, online banking, online social networks, online gaming, fake websites, personal protection, online harassment – Report and Handling Problems – Cyber-Security for higher education – Small business: assess your risk, protect your business, monitor threats, draft and implement Cyber-Security plan – Protect your customers: gain their trust, best practices – Protect your employees: resources, incident reporting – All points from source (3)
Methodology:	– 'NSCA's public facing presence is its website www.staysafeonline.org.' On the website, users can access various links that enable them to learn more about cyber safety(1) – Also made available through social networks: MySpace, Facebook, YouTube, and Twitter (1) – K – 12 Poster and Video Contest – Studies completed and published on the website to help end – users – Videos are available on the website for users (3)
Target Audience:	Children, Parents, College Students, Teachers, and Small Businesses
Evaluation:	Not found
Additional Information:	The National Cyber-Security Alliance exists through a 'public private partnership, working with the Department of Homeland Security (DHS), corporate sponsors (ADP, AT&T, Cisco, EMC, Google, McAfee, Microsoft, SAIC, Symantec), and non-profit collaborators to promote Cyber-Security awareness for home users, small and medium size businesses, and primary and secondary education.'
Sources	1. 'About Us' *National Cyber-Security Alliance* <http://www.staysafeonline.org/content/about-us> (accessed 20 May 2010). 2. 'National Cyber-Security Alliance in Brief' *White House Website* <http://www.whitehouse.gov/files/documents/cyber/National%20Cyber%20Security%20Alliance%20in%20Brief%203%209%2009.pdf> (accessed 20 May 2010).

Item	Notes
	3. 'Site Map' *National Cyber-Security Alliance* <http://www.staysafeonline.org/sitemap> (accessed 20 May 2010).

Campaign 2 – National Cyber-Security Awareness Campaign Challenge

The National Cyber-Security Awareness Campaign Challenge

> 'is a competition to find the most effective and creative plan for education the American public about Cyber-Security.'

Item	Notes
Campaign Name:	'National Cyber-Security Awareness Campaign Challenge', hosted by Safe Internet Alliance and National Cyber-Security Alliance
Organisation:	U.S. Department of Homeland Security and the Safe Internet Alliance-Under the Obama Administration
Main URL:	http://www.dhs.gov/files/programs/gc_1158611596104.shtm#1
Dates:	Application must be submitted before April 29, 2010, the results have not been announced. The campaign is still in process.
Costs:	Not Applicable
Topics covered:	Personal Internet security, and safe practices for personal Internet and computer use
Target Audience:	All United States citizens
Methodology:	– President Obama is reaching out to the public through methods U.S. citizens propose are the most efficient method to spreading the word of Cyber-Security – United States citizens respond to the Challenge by submitting methods they believe will best spread awareness of Cyber-Security threats people face, and how to retain Cyber-Security.
Evaluation:	The results of the campaign have not been published. They will be revealed in October 2010, which is the United States' National Cyber-Security Awareness Month.
Additional Information:	According to the campaign, Cyber-Security is 'one of the most serious economic and national security challenges' the United States must face. The campaign urges citizens to play an active role in securing cyberspace if they wish to ensure the safety of their families and communities online The winners of the challenge will meet with the Department to assist with the National Cyber-Security Awareness Campaign in October. The results of the competition have not been released yet, but will be revealed in October 2010
Sources:	1. 'Cyber-Security: Our Shared Challenge' *Homeland Security* <http://www.dhs.gov/files/programs/gc_1158611596104.shtm#1> (accessed 20 May 2010).

Campaign 3 – Protected Critical Infrastructure Information Program

US-CERT is a branch of the national Cyber-Security Division at the Department of Security.

Item	Notes
Campaign Name:	Protected Critical Infrastructure Information Program (sources a and b)
Organisation:	United Stated Computer Emergency Readiness Team (CERT) – A public – private partnership created by Homeland Security working with 'private sector Cyber-Security vendors, academia, federal agencies, Information Sharing and Analysis Centres, state and local governments, and domestic and international organisations' (1)
Main URL:	http://www.US-CERT .gov/aboutus.html and http://www.dhs.gov/files/programs/editorial_0404.shtm (2)
Dates:	2002 – Present (2)
Costs:	Not found
Topics covered:	– Sharing information between private sectors and the federal government (2) – Done for national security to counter terrorism (2) – Information for Technical Users (Respond to the Latest Threats, Read Latest Security Tip, Useful Publications, Related Resources) - Information for Non – Technical Users (Respond to the Latest Threats Read the Latest Security Tip, Useful Publications, Related Resources) - Information for Government Users (Collaboration groups, Analytical Tools and Programs, Incident – Related Information, Respond to Latest Threats, Current Activity) – Control Systems Security Program (What's New, Top 10, Reporting, Critical Infrastructure News)
Target Audience:	– Technical Users – Non – Technical Users – Government Users
Methodology:	– Legislation passed in 2002 (Critical Infrastructure Information Act) (2) – Annual symposiums and seminars (1)
Evaluation:	Not found
Additional Information:	'US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable Cyber-Security information to the public. Information is available from the US-CERT web site, mailing lists (http://www.us-cert.gov/cas/signup.html), and RSS channels. US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the United States government about Cyber-Security.' This communication is enabled through mailing lists and feeds, and giving he public an opportunity to report an incident of a threat to Cyber-Security, an opportunity to report phishing and any other vulnerabilities.
Sources:	1. 'About Us: CERT' *Homeland Security* <http://www.US-CERT .gov/aboutus.html> (accessed 27 May 2010) 2. 'Protected Critical Infrastructure Information Act' *Homeland Security* http://www.dhs.gov/files/programs/editorial_0404.shtm (accessed 27 May 2010)

Campaign 4 – OnGuard Online

OnGuardOnline 'provides tips from the federal government and the technology industry to help [the public] be on guard against Internet fraud, and provide resources to help the public learn how to secure their computers and protect their personal information.'

Item	Notes
Campaign Name:	OnGuard Online
Organisation:	OnGuard Online with Federal Trade Commission, Naval Criminal Investigative Service, U.S. Department of Education, Department of Commerce, Homeland Security, Federal Deposit Insurance Corporation, U.S. Commodity Future Trading Commission, and a number of other government agencies (a)
Main URL:	http://www.onguardonline.gov/
Dates:	Present (unclear when established)
Costs:	– Unclear; however, receives support from 20 different organizations
Topics covered:	– Overview of safety online – Financial decisions (i.e. Broadband, shopping online, online investing, VoIP services, online auctions) – Personal decisions (Health online. Computer disposal) – Cross – Border Scams – E-mail scams – Identity Theft – Kid's Privacy – Laptop Security – Malware – P2P Security – Phishing – Spyware – Wireless security
Target Audience:	– Elderly – Parents – Adults – Children
Methodology:	– Videos – Literature – Interactive games (such as quizzes to test knowledge of Cyber-Security) – Asking visitors to spread the word by passing out pamphlets and publishing the link to the organization on volunteers' web pages
Evaluation:	Not found
Additional Information:	The site provides an interactive approach to educating users about Internet security. Through games, videos and other tools, people of all ages can learn how to protect their personal information online. The organization encourages users to disseminate information on Cyber-Security by posting links to OnGuard Online, posting games found on the site to one's own site, handing out free publications to friends and family, and involving the media.
Sources:	1. 'Homepage' *OnGuard Online* <http://www.onguardonline.gov/> (accessed 28 May 2010) 2. 'Topics' *OnGaurd Online* <http://www.onguardonline.gov/topics/overview.aspx> (accessed 28 May 2010)

Campaign 5 – United States Postal Inspection Service

This site provides users with guides on how to protect themselves from identity theft and other forms of fraud. It also gives consumers an opportunity tor report any form of fraud with an online application that will be electronically delivered to the United States Postal Inspection Service. The site does not provide users with a mission's statement or objectives.

Item	Notes
Campaign Name:	United States Postal Inspection Service
Organisation:	United States Postal Inspection Service
Main URL:	https://postalinspectors.uspis.gov/
Dates:	Organization established in 1737, but it unclear when the responsibilities of the organization expanded to cover fraud that occurs on the Internet (b)
Costs:	Not found
Topics covered:	– Employment Fraud (franchise fraud, phony job opportunities, pyramid schemes, short – paid postage, postal job scams, work at home schemes, mystery shopper scam) – Financial Fraud (900 telephone number scheme, advance-free loan scheme, charity fraud, credit card fraud, schemes that ask you to pay for free government services, cut – rate health insurance fraud, investment fraud, solicitations disguised as invoices, oil and gas investment fraud, oil fraud) – Fraud Against Older Americans (fraud against older people, sweepstakes advice for the elderly) – Sweepstakes and Lottery Fraud (illegal sweepstakes information, chain letters, free prize scheme, foreign lotteries by mail, government look alike mail, free vacation scams) – Telemarketing Fraud (rules for telephone solicitations, characteristics of telemarketing fraud) – Mail Fraud (home improvement and home repair fraud, phony inheritance scam, receipt of unsolicited merchandise, prison pen pan money order scam, fraudulent health and medical products, removing your name from national contact list) (3)
Target Audience:	– Elderly – Parents – Adults – United States citizens (1)
Methodology:	– Literature online – Complaint line through website
Evaluation:	Not found
Sources:	1. 'Home Page' *United States Postal Inspection Service* <https://postalinspectors.uspis.gov/> (accessed 20 May 2010). 2. 'History' *United States Postal Inspection Service* <https://postalinspectors.uspis.gov/aboutus/ History.aspx> (accessed 20 May 2010). 3. 'Mail Fraud Schemes' *United States Postal Inspection Service* <*https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/FraudSchemes.aspx*> (accessed 20 May 2010).

Campaign 6 – Empowering Consumers: Protecting Privacy (Privacy Rights Clearinghouse)

The Privacy Rights Clearinghouse has two main focuses: consumer information and consumer advocacy. This site offers provides online material on many topics.

Item	Notes
Campaign Name:	Empowering Consumers. Protecting Privacy.
Organisation:	Privacy Rights Clearinghouse
Main URL:	http://www.privacyrights.org/
Dates:	1992 – Present
Costs:	Not mentioned – Funded by the Rose Foundation Consumer Privacy Rights Fund, California Consumer Protection Foundation, Roger L. Kohn Fun, and Consumer Federation of America.
Topics covered:	*Number next to topic notes the number of subtopics within each category. Each subtopic consists of an article related to the category, and links to other privacy institutions. – Privacy Basics (24) – Background Checks and Workplace (31) – Banking and Finance (56) – Credit and Credit Reports (25) – Debt Collecting (9) – Education (4) – Harassment and Stalking (4) – Identity Theft and Data Breaches (47) – Insurance (10) – Junk Mail/Faxes/Email (16) – Medical Privacy (32) – Online Privacy and Technology (57) – Privacy when you shop online (16) – Public Records and Informational Brokers (18) – Social Security Numbers (10) – Telephone Privacy (30) – Additional Readings (11)
Target Audience:	– Parents – General Public
Methodology:	– Ask subscribers to post the site's link on Twitter – Online Literature
Evaluation:	Not found
Additional Information:	The Privacy Right Clearinghouse's goals are as follows: '1) Raise consumers' awareness of how technology affects personal privacy 2) Empower consumers to take action to control their own personal information by providing practical tups on privacy protection 3) Respond to specific privacy – related complaints form consumers, intercede on their behalf, and, when appropriate, refer them to the proper organizations for further assistance. 4) Document the nature of consumers' complaints and questions about privacy in reports, testimony, and speeches and make them available to policy makers, industry representatives, consumer advocates, and the media. 5) Advocate for consumers' privacy rights in local, state and federal public policy proceedings, including legislative testimony, regulatory agency hearings, task forces, and study commissions as well as conferences and workshops.' In an effort to achieve these goals, the Privacy Rights Clearinghouse offers a number of services to citizens throughout the nation. A hotline, which can be found on the site, is offered to people to consumers who would like to report privacy abuses or receive information on privacy protection. The site also provides clients with fact sheets on privacy issues in both English and Spanish. Additionally, the organization hosts a 'referral service,' which allows journalists and policy makers to network with victims of privacy abuses and are willing to talk to the media or testify in legislative and regulatory agency hearings. Lastly, the Privacy Rights Clearinghouse reaches out to the community and businesses by making presentations at conferences, employee training sessions, and civic and community group meetings.

Item	Notes
Sources:	1. 'Home Page' *Privacy Rights Clearinghouse* <http://www.privacyrights.org/> (accessed 20 May 2010). 2. 'Site Map' *Privacy Rights Clearinghouse* <http://www.privacyrights.org/sitemap> (accessed 20 May 2010). 3. 'Privacy Clearinghouse' *Wikipedia* <http://en.wikipedia.org/wiki/Privacy_Rights_Clearinghouse> (accessed 20 May 2010).

Campaign 7 – Working to Resolve Identity Theft

The Identity Theft Resource Centre's mission is to

> 'provide best in class victim assistance at no charge to consumers throughout the United States. Educate consumers, corporations, government agencies and other organization on best practices for fraud and identity theft detection, reduction and mitigation. [Lastly, to] provide enterprise consulting and outsourced services related to information breach, fraud and identity theft.'

Item	Notes
Campaign Name:	Working to Resolve Identity Theft (a)
Organisation:	Identity Theft Resource Center with American National Standards Institute, National Foundation for Credit Counseling, National Cyber Forensics and training Alliance, National Cyber-Security Alliance, California Crime Prevention Officers Association, Securing our eCity, Victim Assistance Coordinating Council, San Diego District Attorney's Victim Assistance Program, San Diego County Board of Supervisors (a)
Main URL:	http://www.idtheftcenter.org/ (a)
Dates:	1999 – Present (c)
Costs:	Not mentioned Sponsored by First Advantage Membership Services, Trend Micro, Fellowes, Uni-ball, ID Analytics, Spamcuaq, Qualcomm, Salesforce.com, Identity Theft 911, Trusted ID, Debix: The Identity Protection Network, Soph Shield, Info Armor: Identity Protection Experts, California Consumer Protection Foundation
Topics covered:	– Victim Solutions (Help! I'm a victim, Letter Templates, Inspirational Thoughts) – Prevention Tips (Consumer guide, ID theft test, workplace FAQ's) – Scams and Consumer Alerts (Scams, specific scam alert, resources and other scam alerts, example of scams) – Teen Space (teen fact sheets, teacher enrichment, sponsors of teen space, ID theft quizzes) – About ITRC (Corporate overview, history, awards and commendation) – ITRC Sponsors (Sponsor Logos and links) - Training and presentations (Presentation/training, past presentations, presenter biographies) – Media resources (Press releases) – Law Enforcement (Victim communications, victim relations, presentation and training) – Business Solutions (workplace facts, consultation services, business IQ test) – Community event (upcoming and past); Pages offered in Spanish and Chinese – State Resources – Identity Theft News – Commendations (b)
Target Audience:	– Parents – Teachers – General Public (b)
Methodology:	– Presentations/Training about Privacy Rights – Community Events
Evaluation:	Not found
Additional Information:	The Resource Center promotes the belief that: 'both consumers and businesses are victims of identity theft and fraud. Prevention and reduction of identity theft will require education and cooperation between consumers, business, law enforcement agencies, and legislators. The ITRC believes that support and education of business has a strong positive impact on the restoration of victims' lives, and the prevention of further identity theft. [Lastly,] the ITRC has consciously avoided legal advocacy as a method of forwarding its mission.'
Sources:	1. 'Home Page' *Identity Theft Resource Center* <http://www.idtheftcenter.org/> (accessed 20 May 2010). 2. 'Site Map' *Identity Theft Resource Center* <http://www.idtheftcenter.org/sitemap.html> (accessed 20 May 2010). 3. 'History' *Identity Theft Resource Center* <http://www.idtheftcenter.org/artman2/publish/a_history/index.shtml> (accessed 20 May 2010).

Campaign 8 – Department of Justice

This site hosts the US DoJ's materials on online and ID fraud.

Item	Notes
Campaign Name:	Fraud (1)
Organisation:	United States Department of Justice: Fraud Section
Main URL:	http://www.justice.gov/criminal/fraud/websites/idtheft.html
Dates:	n/a
Costs:	Unclear, funded by federal government
Topics covered:	Identity Fraud (3) – Most common ways to commit identity fraud or theft – What the Department of Justice is doing about identity fraud – What individuals can do about identity fraud – How individuals can do to avoid identity fraud – What to do if you are a victim of identity fraud – How to find out more about identity fraud
Target Audience:	– General Public – Businesses
Methodology:	– Online Literature – Offers grants to businesses (8)
Evaluation:	Not found
Additional Information:	'The Fraud Section plays a unique and essential role in the Department's fight against sophisticated economic crime. The Section is a front line litigating unit that acts as a rapid response team, investigating and prosecuting complex white-collar crime cases throughout the country. The Section is uniquely qualified to act in that capacity, based on its vast experience with sophisticated fraud schemes; its expertise in managing complex and multi – district litigation; and its ability to deploy resources effectively to address law enforcement priorities and respond to geographically shifting crime problems. These capabilities are an essential complement to the efforts of the United States Attorneys' Offices to combat white-collar crime. The Fraud Section also plays a critical role in the development of Department policy. The Section implements enforcement initiatives and advises the Department leadership on such matters as legislation, crime prevention, and public education. The Section frequently coordinates interagency and multi-district investigations and international enforcement efforts. The Section assists prosecutors, regulators, law enforcement and the private sector by providing training, advice and other assistance. The Section, often in a leadership capacity, participates in numerous national, regional and international working groups. To fulfil its mission, the Fraud Section seeks to build and enhance its most valuable resources by maximizing opportunities for its dedicated professionals. By providing direct supervision, training and mentoring for its attorneys and other professionals, the Section seeks effectively to develop the knowledge, skills and judgment required to fulfil its unique and important mission.'
Sources:	1. 'Home Page' *The Department of Justice* http://www.justice.gov/ (accessed 4 June 2010) 2. 'About the Department of Justice' *The Department of Justice* http://www.justice.gov/02organizations/about.html (accessed 4 June 2010) 3. 'Identity Fraud' *The Department of Justice* http://www.justice.gov/criminal/fraud/websites/idtheft.html (accessed 4 June 2010) 4. 'Mass Marketing Fraud' *The Department of Justice* http://www.justice.gov/criminal/fraud/Internet/ (accessed 4 June 2010) 5. 'Foreign Corrupt Practices Act' *The Department of Justice* http://www.justice.gov/criminal/fraud/fcpa/ (accessed 4 June 2010) 6. 'Documents and Reports' *The Department of Justice* http://www.justice.gov/criminal/fraud/documents/ (accessed 4 June 2010) 7. 'Interagency Working Groups' *The Department of Justice* http://www.justice.gov/criminal/fraud/working-grps/ (accessed 4 June 2010) 8. 'Grants' *The Department of Justice* http://www.justice.gov/10grants/business-opportunities.htm (accessed 4 June 2010)

Campaign 9 – Deter, Detect, Defend: Avoid ID Theft – Federal Trade Commission (FTC)

This is a 'one-stop national resource to learn about the crime of identity theft. It provides detailed information to help [the public] deter, detect, and defend against identity theft…Consumers can learn how to avoid identity theft—an how to help their customers deal with identity theft, as well as how to prevent problems in the first place. Law enforcement can get resources and learn how to help victims of identity theft.'

Item	Notes
Campaign Name:	Deter, Detect, Defend: Avoid ID Theft
Organisation:	Federal Trade Commission (FTC)
Main URL:	http://www.ftc.gov/bcp/edu/microsites/idtheft/
Dates:	Not Applicable
Costs:	Not Applicable
Topics covered:	Consumers – About Identity Theft / – Deter ID Theft / – Detect ID Theft / – Defend against ID Theft / – Filing a complaint with the FTC / – Resolving Specific Identity Theft Issues / – Tools for victims / Businesses – Assisting Victims / – Dealing with Data Breach / – Safeguarding information / – Business Publications / – Resources Law Enforcement - Investigations / – Helping Victims / – Publications / – Laws Military – ID Theft for Military / – Active Duty Alerts / – Tools for Victims Media – Press Release Archives / – How to write about ID Theft Reference Desk – National Data / – State Data / – Reports and Testimony / – Laws / – FTC Rule Making
Target Audience:	– Consumers – Businesses – Law Enforcement
Methodology:	– Online Literature – Complaint Process – Videos – Online quizzes
Evaluation:	Not found
Additional Information:	This organization is a campaign sponsored by the Federal Trade Commission. The site offers visitors informational fact sheets on identity theft, videos on how to retain privacy, a procedure to follow if one is a victim of identity theft, and quizzes that allow people to evaluate their own knowledge about identity theft. The site's primary aspiration is to help people deter, detect, and defend themselves against identity theft.
Sources:	1. 'Welcome to the FTC's ID Theft Website' <http://www.ftc.gov/bcp/edu/microsites/idtheft/> (accessed 5 June 2010).

Campaign 10 – FakeChecks – National Consumers League (NCL)

This site takes an interactive approach to alert civilians about personal Cyber-Security threats, as well as assisting victims to recover from infractions the victim and his family may have suffered from identity theft. Users can test their knowledge about identity theft by taking a quiz, or watch videos about identity theft. Additionally, the site provides videos of interviews with actual victims of identity theft. For further information on identity theft, users can follow links to another site found on FakeChecks.org.

Item	Notes
Campaign Name:	FakeChecks
Organisation:	National Consumer League with: – American Bankers Association / – American Express / – BITS/The Financial Services Roundtable / – Capitol One / – Fifth Third Bank / – Identity Theft Assistance Center / – JP Morgan Chase / – Publisher's Clearinghouse / – Visa / – The Western Union Company / – The National Consumer's League / – United States Postal Inspection Service (b)
Main URL:	http://www.fakechecks.org/about.html
Dates:	Not stated
Costs:	– Funded by donations through the National Consumers League (b)
Topics covered:	– Are You at Risk Tests (At risk from being scammed by a foreign business scheme, overpayment offer, sweepstakes scheme, scammed by scheming suitor, rental scheme, online work at home offer) (c) – Videos (Love Losses, Foreign Business, Sudden Riches, Overpayment, Rental Schemes) (d) – Prevention (Love Losses, Foreign Business, Sudden Riches, Overpayment, Rental Schemes) (e)
Target Audience:	– Consumers
Methodology:	– Fraud Test – Videos – Online Literature – Opportunity to Report ID Theft
Evaluation:	Not found
Additional Information:	The National Consumer's League (NCL), 'the nation's oldest Non-profit consumer organization' established Fakehecks.org in collaboration with the Alliance for Consumer Fraud Awareness, which is 'a coalition of consumer and business organizations, government agencies, and companies that are committed to finding fake check scams.'
Sources:	1. 'Home' *FakeChecks* <http://www.fakechecks.org/index.html> (accessed 5 June 2010). 2. 'About Us' *FakeChecks* <http://www.fakechecks.org/about.html> 3. 'Tests' *FakeChecks* <http://www.fakechecks.org/fraudtest.html> 4. 'Videos' *FakeChecks* <http://www.fakechecks.org/videos.html> 5. 'Prevention' *FakeChecks* <http://www.fakechecks.org/videos.html> (accessed 5 June 2010).

Campaign 11 – Computer, Mobile Phone and PDA Security

Precise Security offers users documents and programs to help protect them against viruses on their computers, mobile phone, and PDA. The site serves as an archive for articles about viruses, and programs that protect consumers against viruses. These articles may be informative of how the software functions, or a review of whether or not the program works well. The organization does not include a mission statement, or philosophy on the research completed on the organization's behalf.

Item	Notes
Campaign Name:	Computer, Mobile Phone and PDA Security
Organisation:	Precise Security
Main URL:	http://www.precisesecurity.com/rogue/Cyber-Security/
Dates:	2006 – 2010
Costs:	Not disclosed
Topics covered:	Main Topics: – Computers (b) – Phones (c) – PDA's (d) (Each category includes hundreds of articles on Cyber-Security for each technological device. Comments can be found under each topic) Sub Categories: – Adware – HackTool – Hijacker – Spyware – Rogue – Trojan – Unwanted Program – Virus – Worm – Files and Process Each subcategory includes hundreds of articles on Cyber-Security for each technological device. Comments can be found under each topic.
Target Audience:	– Consumers
Methodology:	– Literature – Interaction through posts and blogs germane to malware and malware resolutions
Evaluation:	Not found
Sources:	1. 'Home' *Precise Security* <http://www.precisesecurity.com/rogue/Cyber-Security/> (accessed 5 June 2010). 2. 'Computer' *Precise Security* <http://www.precisesecurity.com/blogs/> (accessed 5 June 2010). 3. 'Mobile Phone' *Precise Security* <http://www.precisesecurity.com/mobile-phone/> (accessed 5 June 2010).

Campaign 12 – Bringing Law and Order to the Cyber World

Cyber Top Cops was established in April 2006 in South Africa. It is sponsored by an individual who is passionate about combating cyber crime. His goal is to 'educate people and keep them informed about cyber threats and the latest developments regarding cyber crime. By tackling the root of the problem, namely ignorance, [Cyber Top Cops] hopes to build a cyber community that has wit and is clever enough to survive on its own in the Cyber World.'

Item	Notes
Campaign Name:	Bringing Law and Order to the Cyber World (South Africa)
Organisation:	Cyber Tops Cops – The Cyber-Security Experts
Main URL:	http://www.cybertopcops.com/
Dates:	2006 – 2010
Costs:	Not found
Topics covered:	– Anti-Virus – Anti-Spyware – Anti-Adware – Anti-Hacker – Anti-Spam – Anti-Fraud (Anti-pages include a definition, how one's computer becomes infected, and how to rid themselves of the issue) -Internet Security (what is malware, what kind of software is used to combat malware effectively, what are benefits in an integrated Internet Security Suite?, Where can I find an effective and affordable Internet Security Suite?) – Malware Removal Guide (Conventional Malware Removal Method, Special Malware Removal Tools, Online Malware Scanners, What to do if I am still stuck, ask the malware experts, Final Resort: Generate a HijackThis Log) – Tips and Tricks (15 articles) – Report Cyber Crime (21 sites where cyber crime can be reported) – Free Downloads (10 personal Cyber-Security free downloads) – Call for Backup (40 additional sites) – Cyber Top Cop Online Threat Simulations (actual simulation)
Target Audience:	– Consumers
Methodology:	– Online Literature – Offer software for sale on site
Evaluation:	Not found
Additional Information:	The site includes a plethora of resources for users, such as online literature about cyber threats and links to other sites that provide further information on cyber crime
Sources	1. 'Home Page' *Cyber – Tops Cops* <http://www.cybertopcops.com/> (accessed 5 June 2010)

Campaign 13 – 419 Eater

Scam Eater 419 archives correspondences between 419 scammers and civilians who pose as people interested in the foe opportunity the scammers present. After several exchanges, the civilian reveals his intentions to capture the scammer in the act. At this point, the civilian posts his correspondences on this website to alert other consumers of scams circulating on the Internet. The website defines this practice as scam baiting. The website invites new members to participate in the practice of scam baiting. There is a forum on the website for scam baiters to discuss the practice of scam baiting. The website also provides awards for the 'best' scam baiting e-mails, and any pictures scammers have sent civilians. According to the website, these archives are created to alert and warn consumers of scams circulating on the Internet.

Item	Notes
Campaign Name:	419 Eater
Organisation:	419 Eater
Main URL:	http://www.419eater.com/index.php
Dates:	Not mentioned
Costs:	Not found
Topics covered:	– Letter Archive (Correspondences and information accumulated about individual scams. This information is posted by various individuals onto the site) – Trophy Room (Pictures of actual individuals who attempted to scam others. *Questionable these are reliable photos*) – Hall of Shame (Scammers who sent photo shopped images of themselves to the site) – 419 FAQ (information about 4 – 1 – 9 scams) – Propaganda (artwork by members of the anti-scam community to warn others about scammers) – Links (40 links to other sites) – Forums – Scambaiting Tips – Video Files (Videos of scammers who accomplish 'fake feats' in an effort to collect money. Not yet available) (all links available from home page in top bar)
Target Audience:	– Consumers
Methodology:	– Literature – Videos – Forums
Evaluation:	Not found
Sources:	1. 'Home' *419 Eaters* <http://www.419eater.com/index.php> (accessed 5 June 2010).

Campaign 14 – Fraud Aid

Fraud Aid aspires to 'provide support and guidance for fraud victims and their families worldwide; to serve as a deterrent to fraud everywhere; to spread easy-to-understand fraud awareness, recognition, and prevention education throughout the world community and to develop efficient tools and support systems for law enforcement, public and private investigators, fraud examiners, fraud attorneys and defence attorneys.'

Item	Notes
Campaign Name:	Fraud Aid
Organisation:	Fraud Victim Advocacy
Main URL:	http://www.fraudaid.com/advocacy.htm
Dates:	Not mentioned
Costs:	Not found
Topics covered:	– The Store: Spyware Beware! (Computer security products for family, children, home, wireless and business; practical, easy to understand explanations of malicious computer invasions and the software that protect you from them) – Identity Theft (what you and a murderer may have in common: your identity, all of your Internet activity is on your hard drive, where your information goes, your bad credit doesn't matter, after proving your identity) – Firewalls and backdoors (what is a backdoor, about spyware, Trojan horses, worms and viruses, chat and e-mail logging, how to buy computer protection) – Backstage (the script, motivation, profile of a con artist, how con artists scheme to set up their victims, what a con artist won't tell you, what a con artist will tell you, how can I b sure I've been conned?, where is my Money?, money – laundering) – Victims (The Fraud Victim's Manual, how to organize and write a report to law enforcement, jurisdictions, wire transfer systems, know your Miranda rights and how to use them) – Scam Speak (Fraud Tales, 419 Counterfeit check scam, payment processing scam, payment processing scam letter database, 419 Nigerian Letter scam, hidden facts about 419 letters, Nigerian scam letter free online database) – ScamSpam (Lottery, welcome to the Free online lottery/lotto scam letter database!, Bill Gates and the Lottery, free online lottery scam letter database search, group lottery vs. lottery scams, how to use world time zone map, international lotteries vs. lottery scams, lottery scam letter samples from the online database, sponsored vs. operated lotteries, forged fraud – aid email database, welcome to the online database of forged fraud – aid emails)
Target Audience:	– Consumers
Methodology:	– Literature
Evaluation:	Not found
Additional Information:	In an effort to achieve this goal, the organization provides online literature on the website, and also has a volunteer program to assist victims of fraud. There is a wide range of tasks volunteers can choose to pursue, ranging from technical support and budgeting, to assisting victims of fraud. Those who assist victims of fraud are known as Fraud Victim Advocates. According to the site, a Fraud Victim Advocate 'guides the fraud victim and/or the fraud victim's family for as long as it takes to work through the consequences of the crime perpetrated on them.'
Sources:	1. 'Home' *Fraud Aid* <http://www.fraudaid.com/advocacy.htm> (accessed 15 June 2010). 2. 'Site Map' *Fraud Aid* <http://fraudaid.com/site-map.htm> (accessed 15 June 2010).

Campaign 15 – Wired Safety

Wired Safety offers a plethora of resources for Internet users on how to remain safe online. The site covers a range of topics from social networks to cyber bullying and identity theft. A user can watch a video, read information, or learn more from free classes offered by trained volunteers. There are other research and training activities offered online.

Item	Notes
Campaign name	Wired Safety
Organisation:	Wired Safety
Main URL:	http://www.wiredsafety.org/
Dates:	1995 – Present
Costs:	Not found
Topics covered:	– Cybercrime (Hacking, Identity Theft, Missing Kids, Spam, Cyberstalking, Free Speech, Identity Theft, Kids, Privacy, Scams, Spam, Technology – Cyberlaw (Child Pornography. Copyrights, Cyberstalking, Free Speech, Identity Theft, Kids, Privacy, Scams, Spam, Technology – New to the 'net? (Read our Internet 1010) – Want to Learn More? (Sign up for out classes) – Cyberstalking and Harassment (Definitions, support, and help) – Internet Predators (What we all need to know) – Is Your Child at Risk? – Need help now? (Our Cyber 911 help line for victims of cyberabuse) – Kids Online (Information just for kids, tweens, and teens) – Spyware and Adware (how to detect and remove spyqare) – Email Safety (Information on spam, scams and chain letters) – Chatting Online (chat and IM safely and learn the lingo) – Online Gaming Safety – Downloading Music Safely (What the law says and disabling P2P – Identity Theft (How safe is your personal data? – Online and Cyberdating (How to have fun and stay safe) – Online Shopping and Auctions (Advice on safer e-commerce) – Scams and Fraud (how to tell a hoax and report an online fraud) – Website Safety and Policies (Building a Safer Website) – Blog and Diary Web Sites – Cell phones – IM and SMS text messaging – Cyber Bullying – Identity Theft
Target Audience:	– Media – Parents – Educators – Law Enforcement – Kids, Tweens and Teens

Item	Notes
Methodology:	– Online literature and videos – Interactive courses for Internet users – Trained Volunteers (Divisions listed below with descriptions as found on site) – Site Team and Research Team (Wired Safety Safe Sites. Finding safe and fun links for families. Rating sites for software filtering products. – Internet Relay Chat Division (Channel Operators – they help to keep the peace, and provide help for visitors on many topics, ranging from victims of cyberstalking to Internet questions. – Web Support Team (The Web Support Team directly assists the Web Team and includes HTML coders, graphic artists and HTML – savvy translators for our Web site and database folks.) – Law Enforcement Team (Our law enforcement volunteers...and technology investigation skills...get a Wired Safety Certification. Only current or retired law enforcement officers, Corrections officers, and Federal law enforcement officers. – Strategic Alliances (This group covers a lot of territory – from fundraising, to increasing awareness of our services with online providers, computer companies, Internet portals etc. We really need your help here to keep Wired Safety running!) – International Division (Our volunteers come from all over the world. This division is working on translating our site to many different languages. Members of this team work to recruit volunteers as well as raise awareness of Internet safety and help in their own respective countries.) – Wired-ed (Our online education program. These are our instructors and our writers. They teach the classes, keep the attendance for members, write new classes...busy busy group!) – WiredBuddies (Seasoned Wired Safety members of at least 3 months that walk the New Applicants through the first steps of the Wired Safety. – Child Exploitation Division (This team works to get rid of child pornography on the Internet. It is a part of the larger Cyberstalking and Harassment team Division, and a police letter is required.) – Wired Safety Kids Team (Mentors who want to help kids put together a great website should sign up here!) – Cyberstalking and Harassment Team (Cyberstalking and harassment is a special division available on an invitation only basis. Once you have completed the requisite training) – Teen Angels (Teens between 13 and 17 build a fun and safe place to 'hangout', teach the younger kids, and learn important skills. This is a quickly growing group – there is a lot to do helping to monitor our safe chat channel, teaching classes just for kids on the Internet safety, and working on building a fantastic monthly e-zine aimed just at teens!)
Evaluation:	Not found
Additional Information:	A person who wishes to become a volunteer must be very committed. The individual must send a clearance letter from their local police department to the organization. Once they are cleared, they must attend informational classes in Instant Relay Chat and complete them in 90 days or less. The three primary initiatives for volunteers are as follows: – Safety and technology education – Providing help to law enforcement and Internet users – Protecting the innocent online.
Sources:	1. <http://www.wiredsafety.org/information/overview.html> (accessed 15 June 2010).

Campaign 16 – Cyber Law Enforcement

Cyber Law Enforcement 'is a network of law enforcement officers who specialise in cybercrime investigation, training other law enforcement officers and assisting cybercrime victims online.

Item	Notes
Campaign Name:	Cyber Law Enforcement
Organisation:	Cyber Law Enforcement
Main URL:	http://www.cyberlawenforcement.com/
Dates:	Not found
Costs:	Not disclosed
Topics covered:	– Who we are (Name: of Executive Director) – Our Missions (educate police officers worldwide about cybercrime and cyberlaw, investigative techniques) – Online education (for victims of cybersstalking, cyberharassment, paedophiles, hacking, and virus attacks, and to support groups and online counseling)
Target Audience:	– Law Enforcement Officers – Attorneys – Cyberspace Law Experts
Methodology:	– Training provided for attorneys and law enforcement if they would like to become a member – Training provided for law enforcement officers not looking to be involved in the program – Links for additional information o Cyber-Security and safety – A link that allows Internet users to report cyber crime
Evaluation:	Not found
Additional Information:	[The] tip line handles child pornography, cyberstalking and missing children tips, as well as tips for cyberscams and fraud online. Cyber Law Enforcement also includes Legal Eagles, a group of prosecutors, defense counsel and legal experts in the field of cybercrime, to help educate and guide the Internet community on crime prevention and reporting of cybercrimes.' Cyberlaw Enforcement has four goals: '1) To unite police officers worldwide and educate them on cybercrime, cyberlaw, investigative techniques and how they interact. 2) To provide investigative assistance to police departments when requested. 3) To provide online help and education for victims of cyberstalking, cyberharassment, paedophiles, hacking, and virus attacks, as well as access to support groups and online counselling. 4) To standardize relations and communication between police departments, Internet Service Providers, Legal system contacts and victim advocacy groups worldwide.' If volunteers or law enforcement officers would like to receive training, they must complete an application process.'
Sources:	1. 'Home' *Cyber Law Enforcement* <http://www.cyberlawenforcement.com/volunteer.html> (accessed 15 June 2010).

Campaign 17 – Stop Badware

StopBadware works to 'fight back again viruses, spyware and other badware.' It offers guidelines and other material setting out how to deal with 'badware'.

Item	Notes
Campaign Name:	Stop Badware
Organisation:	Stop Badware with Google, PayPal, and Mozilla and sponsored by MySpace
Main URL:	http://www.stopbadware.org/
Dates:	Not mentioned
Costs:	Receives donations
Topics covered:	– Get involved (Prevent badware, remove badware, report badware, share your story, help others, track badware trends, stay connected) – About StopBadware [sic] – Who We Are (staff, board of directors, working group, our community, partners) – What We Do (Badware website clearinghouse, stop badware stories, community, badware alerts, research publications) – What is badware? (How can I avoid badware?, how can I get rid of badware?, how can I make informed decisions about downloads?, how can I help?, our software guidelines) – FAQ (– Badware Clearinghouse (All topics available from left bar on home page)
Target Audience:	– Internet Users – Website Owners – Software Producers
Methodology:	– Provides online literature and guidelines on how to prevent and treat badware
Evaluation:	Not found
Additional Information:	StopBadware encourage consumers to join their effort through a five-step process. 1) Individuals should prevent or remove badware on their computers. 2) Users should clean and secure their website to protect their website's visitors. 3) Consumers should report a badware URL to the Clearinghouse. 4) Users should learn from and contribute to Stop adware's online community, BadwareBusters.org. 5) Users should share their experiences with badware through StopBadware Stories. Additionally, StopBadware 'cultivates a network of individuals and organizations that share a common goal of eliminating viruses, spyware, and other bad software … by fighting badware, StopBadware and its constituents are helping to build a world in which people are the masters of their own machines. In this world, [consumers can] make informed decisions about how and when hardware, software, and network connections are used.' StopBadware was established 'at Harvard University's Berkman Center for Internet & Society under the direction of Berkman faculty co-directors Prof. Jonathan Zittrain and Prof. John Palfrey. In January 2010, StopBadware became a standalone Non-profit organization. Several prominent technology companies, such as Google, PayPal, and Mozilla, support the organization. (See Partners.) The board of directors consists of experts like Prof. Palfrey and Internet pioneers Vint Cerf and Esther Dyson.'
Sources:	1. 'Home' *Stop Badware* <http://www.stopbadware.org/home/index> (accessed 15 June 2010).

Campaign 18 – National Initiative for Cyber-Security Education (NICE)

The National Initiative for Cyber-Security Education (NICE) was established to build a 'cyber savvy nation' through training, awareness, through post-graduate educational programs, and professional development for federal security professionals.

Item	Notes
Campaign Name:	The National Initiative for Cyber-Security Education (NICE)
Organisation:	National Institute of Standards and Technology
Main URL:	http://csrc.nist.gov/nice/
Dates:	Page created May 11, 2010; Last Updated May 27, 2010
Costs:	Not mentioned
Topics covered:	– Awareness (Mission: to boost national Cyber-Security awareness) – Education (Mission: Bolster formal Cyber-Security education programs) – Workforce Structure (Mission: Ensure that federal agencies can attract, recruit, and retain Cyber-Security employees) – Training & Professional Development (Mission: Intensify training and professional development programs for the existing Federal Cyber-Security workforce)
Target Audience:	– Children – Young Adults – Adults – Federal Workers
Methodology:	– Online Literature – Events – Referral to other helpful websites
Evaluation:	Not found
Additional Information:	'The National Initiative for Cyber-Security Education (NICE) is an ongoing program to teach Americans sound Cyber-Security practices. NICE evolved from the Comprehensive National Cyber-Security Initiative as its scope expanded from a federal government focus to a national one. The program's goal is to enhance the security of the country, and it also will improve computer security in the workplace and at home, as well as prepare future employees in the Cyber-Security workforce. The education initiative ranges from kindergarten to graduate school, and to the public and private sectors. It also includes workforce training and professional development that will provide Cyber-Security training for personnel working, or planning to work, for the federal government.'
Sources:	1. 'Home' *National Institute of Standards and Technology* <http://csrc.nist.gov/nice/> (accessed 14 June 2010)

Campaign 19 – GetNetWise

'GetNetWise is a public service brought to [consumers] by Internet industry corporations and public interest organizations to help ensure that Internet users have safe, constructive, and educational or entertaining online experiences. The GetNetWise coalition wants Internet users to be just 'one click away' from the resources they need to make informed decisions about their and their family's use of the Internet.'

Item	Notes
Campaign Name:	GetNetWise [sic]
Organisation:	GetNetWise [sic] with Google, Microsoft Corporation, Verizon, Adobe, American Library Association, AOL, Center for Democracy & Technology, Comcast, Yahoo!, Council of Better Business Bureaus, TRUSTe, Call for Action, The Children's Partnership, Consortium for School Networking (CoSN), Consumer Action, New Family News, Privacy Rights Clearinghouse (1)
Main URL:	http://www.getnetwise.org/
Dates:	1999 – 2008
Costs:	Not found
Topics covered:	– About Kids Safety (Safety Guide, tools, reporting trouble, kid sites, search, glossary, questions, join us) – Spam (Tips, Tools, Take Actions, Search, Glossary, Questions, Join Us) – Security (Tips, Tools, Take action, search, glossary, questions, join us) – Security (Browsing, shopping, communicating sharing, video tutorials)
Target Audience:	– Children – Parents
Methodology:	– Online literature – Video tutorials – Referrals to other links users the opportunity to present the GetNetWise icon on their social network sites – Offers users the option to send e-mails to their friends (a template already written and found on website) (e)
Evaluation:	Not found
Additional Information:	'GetNetWise is a project of the Internet Education Foundation… GetNetWise is more than a Web site. It's a Web-wide partnership. It includes, through [GetNetWise's] corporate partners, many of the Net's most well – known, trusted, and popular portals and content providers, all of whom are committed to providing Internet users with valuable information and tools. Many organizations and individuals with expertise in online child safety, privacy, security and spam issues provided valuable assistance developing GetNetWise.'
Sources:	1. 'Home' *GetNetWise* http://privacy.getnetwise.org/ (accessed 16 June 2010). 2. 'GetNetWise Supporters' *GetNetWise* http://www.getnetwise.org/about/supporters/ (accessed 16 June 2010). 3. 'Security' *GetNetWise* http://security.getnetwise.org/ (accessed 16 June 2010). 4. 'Privacy' *GetNetWise* http://privacy.getnetwise.org/ (accessed 16 June 2010). 5. 'Spread the Word' *GetNetWise* http://base.getnetwise.org/join/ (accessed 16 June 2010).

Campaign 20 – Fraud Watcher International

Item	Notes
Campaign Name:	Fraud Watchers International
Organisation:	Fraud Watchers International
Main URL:	http://www.fraudwatchers.org/
Dates:	2003 – 2010
Costs:	Not found
Topics covered:	– Phishing Alerts – Business Solutions – Consumer (Consumers home, FWI membership) – Report Fraud (Report Fraud) – Fraud Education (Internet Fraud Home, Know Lottery Scam Operatives) – Identity Theft – Nigerian 419 Scams – FAQ's – Online Auction Fraud – Shopping Online Safely – Privacy on the Internet – Internet Fraud – Where to report it – SPAM – Where does it come from and how to prevent it – Fake Jobs (Money Mules) – Resources
Target Audience:	– Businesses Solutions – Consumers – Members
Methodology:	– Hotline to remove phishing from computer: 1(415) 200 – 0621 – Membership to access additional materials – Online literature – Links to various blogs
Evaluation:	Not found
Additional Information:	'The aim of FraudWatchers.Org is firstly to provide support, guidance and assistance to victims of fraud. We are aware of the circumstances under which people fall prey to these crimes – quite often it is out of the simple, human desire to have a second income, or to help a 'charity' in Africa or maybe it is just the result of buying something on the Internet for your children. *We understand* – it is not always blind, mindless greed that causes fraud victims. *We care* – we have seen hard cases before and we always try our best to look after them. *We know* – we co-operate with police forces all around the world and can guide you to the right people to report your case ... Secondly, we aim to educate people about fraud on the Internet, in all its manifestations. If people are educated about fraud, then the fraudsters and scammers would not have the victims to finance their criminal activities. ... At the last estimate in 2003, there were estimated to be around 300,000 professional scammers operating out of Africa alone, generating over 5 billion scam emails. This is a problem we can fight only with education. You can help us, by educating yourself so that you can educate your family, your friends, and your colleagues. ... We have news items, articles, links, everything you need to help yourself and those you care for.'
Sources:	1. 'Home' *Fraud Watch International* <http://www.fraudwatchers.org/> (accessed 16 June 2010).

Canberra
Purple Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 44
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899
TTY 03 9963 6948

Sydney
Level 15 Tower 1
Darling Park
201 Sussex Street
Sydney NSW

PO Box Q500
Queen Victoria Building
Sydney NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799

acma research

www.acma.gov.au