



***Raising Citizen Awareness
Of Information Security:
A Practical Guide***



**Raising Citizen Awareness of Information Security:
A Practical Guide**

by

Steve Wooding, Aarti Anhal and Lorenzo Valeri

September 2003

***e*Aware**
★

Contents

Introduction.....	1
Why Information Security Awareness?.....	3
What is This Guide for?.....	3
What Is Information Security?.....	4
Different Audience, Different Viewpoints.....	4
Problems in the Virtual World.....	4
Personal Computing.....	4
Connection to the Internet.....	5
E-mail.....	6
World Wide Web.....	6
e-Commerce.....	7
Chat.....	7
Wireless Networks.....	8
Mobile Phones.....	8
Before You Start.....	8
Partners.....	9
Who Are You Talking To? What Is the Message?.....	10
Sample Messages.....	11
Sample Audiences.....	12
Getting the Details Right.....	12
Research Your Audience.....	12
Message Contents.....	12
Technical Level of Information.....	13
Bear in Mind Competing Messages and Risks.....	13
Comparisons with the Real World.....	13
Reaching Your Audience.....	13
Inclusiveness.....	13
Engaging Your Audience.....	14
Resistance to Spending Money.....	14
Spreading the Word – Getting Publicity.....	14
Press Releases.....	14
Interviews.....	15
Other Places to Get Coverage.....	15
Facilities for the Press.....	15
Checking it Worked.....	16
Annex: Methods of Communication.....	19

Introduction

Information and Communication Technologies (ICT) are becoming increasingly important for Europe's citizens, who are all becoming dependent on the use of information networks and services in their daily lives. Yet, while uptake of new technology amongst citizens is high, a large proportion of the European Community's citizens remain unaware of their exposure to risks from security breaches and 'cyber-abuse' in the form of network disruptions, malicious code, criminality and hacking, as well as hardware and software failures. There is an urgent need for the development and implementation of awareness-raising campaigns targeted at citizens to promote the safe and responsible use of ICT.

The e-Awareness for Europe: Digital Awareness and the Security of the Citizen in Europe (eAware)¹ Project, which was funded by DG Research & Technological Development (RTD) under the 'Improving Human Research Potential and the Socio-economic Knowledge Base' programme of the Fifth Framework Programme, aims to inform and educate European citizens about their rights and responsibilities relating to the use of ICT in their daily lives. Through its work, eAware² supports the dissemination of the 2002 Organisation for Economic Co-operation and Development (OECD) *Guidelines for Security of Information Systems and Networks: Towards a Culture of Security*.

Raising Citizen Awareness of Information Security: A Practical Guide provides a 'how to' guide for organisations seeking to launch an awareness-raising campaign in the field of information security. It represents the culmination of a number of the phases involved in eAware's work.

The first phase comprised a literature review and global assessment of current awareness-raising campaigns in the field of information security. This resulted in a comprehensive analysis of good practice in information security awareness-raising, based on a comparative review of over 10 campaigns in over five countries.³ Read in conjunction with this Guide, this report provides invaluable background information on the current environment for both the theory and practice of information security awareness-raising.

The second phase of work involved the implementation by eAware Consortium partners of the best practices found in the course of the global review during a series of national awareness events, which were organised in their respective Member States. These events were targeted at different sections of civil society, e.g. teachers, parents, media, etc and used a number of different techniques to inform and educate the invited individuals and groups.⁴

Having tested these best practices at the events and evaluated their contribution to the success of the national awareness events, it has since been possible to develop an awareness-raising strategy combining the essential elements required to create an effective campaign that successfully achieves its aims. This strategy is now contained in this Guide.

For organisations seeking to launch an awareness-raising campaign, this Guide provides both the strategy and content for any campaign. It begins with an outline of the technologies that are used by the public and, consequently, serve as targets for abuse. A discussion follows of the risks that

1 HPRP-CT-2002-00008.

2 eAware is led by RAND Europe (the Netherlands) and includes the following partners: Intellect (UK), Research Centre – Athens University of Economics and Business (Greece), CLUSIT – Associazione Italiana per la Sicurezza Informatica (Italy), Danish Technological Institute (DTI) (Denmark), TimeKontor AG (Germany), Electronic Commerce Platform Netherlands ECP.NL (the Netherlands), Praxis Centre for Policy Studies (Estonia), INFOLAB (Poland), Universitat Politècnica de Catalunya – EsCERT (Spain).

3 Aarti Anhal, Shawna Gibson and Lorenzo Valeri (2003) 'Promoting Information and Network Security Awareness Among Citizens: A Global Report and Lessons Learned', RAND Europe MR-1775-EC, April. The document is freely available at <http://www.eaware.org>.

4 Further information on the individual national awareness events can be found at <http://www.eaware.org>.

affect particular technologies and the practical means by which such risks can be countered. The final part of the Guide provides a step-by-step manual of the issues to be considered when developing an awareness-raising campaign, and the techniques to be used in order to maximise the impact of efforts made as part of that campaign.

This Guide is of considerable benefit to a variety of audiences involved in awareness-raising, education and public relations in the field of information security. These include:

- public sector organisations:
 - governments;
 - international organisations;
 - consumer organisations;
 - educational establishments;
- private sector organisations;
- computer security organisations; and
- public relations/marketing professionals.

For more information about this Guide and/or the work of the eAware project, please contact:

Lorenzo Valeri
RAND Europe – Berlin
Uhlandstrasse 14
10623 Berlin
Germany
Tel: + 49 (30) 31 01 91 43
Fax: + 49 (30) 31 01 91 19
E-mail: lvaleri@rand.org

Why Information Security Awareness?

Information and Communication Technologies (ICT) provide opportunities that would have astounded our grandparents – continuous access to the latest news and information, the ability to stay in touch with loved ones from any part of the globe, or the option to buy things from thousands of miles away, 24 hours a day.

Unsurprisingly, as with any technological advance, these amazing possibilities also bring new risks and problems with them, including those relating to uncertain identity. For example:

- how do I know the site offering an amazing deal on garden plants is a real business?
- how do I know that my new friend from the Internet chatroom really is a gardener from the south of France?

The use of computers, mobile phones and the Internet is widespread and increasing rapidly; but many people are not sufficiently aware of the risks that they face, or how they can protect themselves online. Some of these technological risks are new: for example, home computers can be hijacked in order to attack other computers on the Internet. Other risks are simply extensions of old ones: credit card fraud has been around as long as credit cards themselves, but now stolen card details can be used across the world within minutes.

In order for people to get the maximum benefit from ICT they need to understand both how to take advantage of technology's benefits, and equally importantly, how to avoid falling victim to the risks that it brings. When communicating this message it is important not to be alarmist – it is important to put risks in the context of the real-world experience of your audience – for example, it is useful to compare the risks of online fraud with the risks of 'real-world' credit card fraud. To avoid being alarmist, or portraying a negative view of technology, you may wish to avoid focusing exclusively on risks in your campaign. Equally, you should avoid overselling any solutions that you suggest as being perfect and 100% effective.

To run a compelling public awareness campaign, you must have a message that is relevant to your target audience and that fits with their interests and motivations. You cannot view 'the public' as a uniform collection of people: different groups have different interests, watch different TV programmes, and obtain their information from different sources, so they have to be approached in different ways. Approaches to communication that engage your audience – responding to their views, worries and concerns – will have greater effect. Of course, such approaches will require greater resource investments.

What Is this Guide for?

This Guide is an introduction to the issues that you may face when trying to raise public awareness about information security.

Many of the issues surrounding public awareness of the safe and responsible use of ICT are similar to those that have been dealt with in the fields of health education and public understanding of science and technology. Consequently, these fields can provide good examples and models of effective practice.

The Guide is structured as follows. First, it provides an overview of the main issues raised by the use of ICT for non-specialist users. Second, it illustrates the steps you will need to think about in order to run a successful awareness-raising campaign:

- beginning with planning;
- working through implementation; and
- ending with how to assess, if the campaign worked.

The Annex to this Guide lists many of the specific methods that could be employed in an awareness-raising campaign and briefly outlines their main advantages and disadvantages.

What Is Information Security?

Information security involves a wide range of technologies: from personal computers with broadband Internet connections, to mobile phones and PDAs (personal digital assistants). Each technology provides its own range of opportunities and risks. This introduction concentrates on computer-related risks, beginning with an overview of the general types of risk before moving to specifics. It covers computers through to online technologies and finally touches on mobile phones.

When dealing with information security, it is important not to overemphasise the technical aspects of security: for example, there is no point in having a long password with letters, numerals and punctuation, if the user has to write it on a note in their desk drawer to remember it. Small-scale surveys have shown repeatedly that most office workers will reveal their passwords to market researchers. Indeed, ex-hacker-turned-security consultant Kevin Mitnick obtained much of the information that he used to exploit computer systems through fast-talking, or ‘social engineering’, rather than through technical means. Similarly, having a hard-to-guess password for your e-mail account does not make your e-mails any more secure when they are passing across the Internet to your correspondent.

Human and social factors are particularly important when helping children to get the most out of the Internet, while minimising the risks involved. Software blocking access to inappropriate web content is available, but such software will never be foolproof. This means that it is vital that children are happy to inform their parents of any problems that they may have encountered online, rather than feeling that they themselves are to blame. Measures such as placing the computer in a public area of the house, and agreeing a ‘family internet policy’ can assist in creating such an environment.

Different Audience, Different Viewpoints

Remember that different audiences will place different emphasis on different risks. On the one hand, parents are likely to be concerned about their children coming across inappropriate material, such as pornography, or about being befriended by strangers in Internet chatrooms. On the other hand, young adults may be far more concerned about the privacy of their personal communications and the security of their credit card details when they shop on the Internet. People’s concerns may stem from personal experience, what they have seen in the newspaper or have been told by friends, hence their ranking of threats may not coincide with that of information security professionals.

Problems in the Virtual World

Many of the risks in the virtual world arise because this environment lacks many of the social cues that we take for granted in the real world. In the real world we tend to meet people through friends, or in familiar places such as the local bar or sports club. We judge people by their appearance, manner and body language. Introductions in the online world lack many, or all, of

these cues. Online, it is almost impossible to know who someone really is: they could be the old-age pensioner they claim to be, or they could be a rebellious teenager playing with an alternative identity.

Personal Computing

Owning a computer brings two principal risks:

- (1) that it will be infected with a virus or by other malicious software; and
- (2) that the computer hardware will go wrong.

Viruses make your computer do what the author of the virus wanted, rather than what you want. They can even delete all of your files or erase your entire hard drive.

Once you are using your computer for anything important, an essential thing to do is to keep back-ups. This way, if the computer does suffer the effects of a virus or you accidentally delete your files, you still have copies in a safe place. If you use the computer only for word processing, a simple back-up strategy would be to keep printed copies of all your documents. The problem with this solution, however, is that you would have to retype any document you wanted to use again if your computer did malfunction. For this reason, a better back-up strategy is to save a copy of each of the individual files on floppy disk or CD-ROM. You can buy special software to make copies of all your important files on CD-ROM; the software ensures that each file is backed up again if it is modified.

Because they are relatively easy to lose, it is particularly important to keep back ups of handheld computers and PDAs. In the workplace, back-ups will normally be taken care of by the IT department, possibly without the users' knowledge. At home, it is up to the individual to assume responsibility for this task.

Connection to the Internet

Connecting your computer to the Internet provides all manner of opportunities and access to endless quantities of information. It also exposes your computer to attacks from malicious hackers. This risk is greatly increased if the computer is attached to the Internet via an 'always on' broadband connection. Malicious hackers can use vulnerabilities in the computer's operating system to take control of your computer. As these vulnerabilities are discovered, manufacturers release software updates (patches) to fix them. Therefore, keeping your software up-to-date is an important first step in computer security. Special software, called a 'firewall' is also available to provide additional protection.

Proving your identity in the real world generally involves your handwritten signature or photo identification. At present, neither of these are used widely in the virtual world. Instead, the virtual world relies on passwords. Consequently, good password practice is an important aspect of information security awareness.

Some important aspects to be aware of are as follows:

- never use passwords that are names or words that can be found in a dictionary;
- always use passwords that include upper and lower case letters and numbers – if the system allows it, you should also include punctuation marks;
- the longer the password, the better – generally nine or 10 characters are sufficient;
- do not use the same password for every service for which you sign up – discovery of the password would compromise all those services you use;

- protect your passwords either by memorising or encrypting them – never write them down; and
- most importantly, keep your password to yourself – strong passwords are of no use if you tell them to other people.

A final, less technical risk, is the ease with which using the Internet could run up high telephone bills or Internet Service Provider (ISP) access charges. Although these charges can be a significant disincentive to Internet use, techniques for minimising them are often neglected in technical discussions of information security.

E-mail

Many people are unaware that e-mails sent across the Internet are only as private as postcards, because they can be intercepted easily and read en-route. In most cases, e-mails are vulnerable because they are not encrypted. Because of this, it is possible for malicious individuals to read other people's private electronic correspondence. While organisations will often keep archives of all e-mails that are sent and received, they should only access this archive in line with the relevant national law and data protection guidelines. Blanket monitoring of e-mails by ISPs is illegal unless specific legal processes have been undertaken. If you would like more information on this aspect of Internet privacy, contact your local law enforcement representatives and/or data protection commissioner.

'Spam' e-mail – the electronic equivalent of junk mail – is a growing problem. Whereas junk mail is only an irritation, spam e-mail often contains unpleasant or obscene material, and can carry viruses.

Important issues that people should be aware of regarding spam e-mail are as follows:

- they should never reply to a spam e-mail (or ask to be 'removed' from the mailing list) – this just confirms that they are a real person;
- they should also bear in mind that the 'From:' address on spam is likely to be fake;
- spammers collect many e-mail addresses by scanning websites and newsgroups – to avoid spam, people should refrain from revealing their e-mail address in such places; or have a different 'private' address that they only reveal to friends and family.

There are also various programmes that will attempt to filter e-mail to remove spam. However, since the filters cannot be perfect, some spam will get through and some legitimate e-mail will be blocked.

Some spam e-mails attempt to entice the recipient into participating in fraudulent schemes – such as the 419 Nigerian scam, or pyramid selling schemes – but although the method of recruiting victims is different, many of these scams predated the arrival of e-mail.

These days, e-mail attachments are a common means of receiving computer viruses. It is important to understand that most of the e-mail virus warnings you receive from friends, acquaintances and work colleagues will be hoaxes – warnings for which there is no virus – and that forwarding these hoaxes wastes time and spreads unnecessary worry.

World Wide Web

Many people see the world wide web as synonymous with the Internet, and web browsing is one of the principal reasons that people connect to the Internet. The web provides a huge quantity of information, which comes in an equally wide range of qualities and from a similarly wide range of sources: some from trustworthy sites and some from areas that are of dubious accuracy. Because of this range of quality it is important to know how to assess the reliability of information on the web.

As well as misleading and incorrect information, there is much that might be considered offensive or inappropriate for certain audiences, such as children. Software which can be controlled by the user or parent is available to block such material, acting as a form of automated censorship. Unfortunately, such software is never perfect, partly because there is no central authority on the Internet to impose a ratings scheme, such as that used by the film industry. The absence of a ratings scheme and the vast size of the Internet means that filtering software inevitably allows access to some material that should have been blocked and blocks access to some material that should have been allowed.

Many web surfers may be unaware of the extent to which their movements around the web are being monitored. At work, employers are likely to keep a record of every web page that their employees view on company computers, and may search this record for inappropriate websites and content. Many ISPs monitor and record the addresses of websites visited by their subscribers. Furthermore, many website publishers will ask users to register, so they can then track and archive information about which pages in a site a browser views over many visits, in addition to observing the adverts on which they click.

e-Commerce

Buying things on the web allows for the possibility of the risks discussed above to extend to your bank or credit card account, and so requires extra care. Judging whether a site is trustworthy becomes especially important when shopping on the web. In the case of payment, it is crucial that credit card details are encrypted when sent across the web, so it is important for consumers to be able to tell whether this is happening or not. In certain web browsers, such as Microsoft Internet Explorer or Netscape Navigator on Windows, this form of encryption is signified by the symbol of a yellow padlock on the bottom of the right side of the browser window. If you are using a different browser, it is possible that the symbol of the padlock will be absent. However, if the URL of the website you are accessing starts with 'https://', this is an indication that personal and financial data are being transferred securely.

Credit card fraud was around long before the advent of the Internet, and much current credit card fraud is still carried out offline. Checking your credit card bills for unexpected expenditure remains good advice, whether you use your credit card for shopping on the Internet or not. Even if your credit card details are used fraudulently on the Internet, they could have been stolen when you dined in a restaurant or stayed at a hotel: they were not necessarily stolen when you were shopping on the Internet.

Online banking raises similar issues (password management, vigilance when on the website, monitoring of statements), but is also slightly different from online shopping. Although commercial sellers on the Internet range from the large established organisations that are concerned with brand and, therefore, security, to smaller outlets that place less value on security measures, all financial organisations that interact with their clients on the Internet value security. Banks are aware of the fact that they are judged by clients on their ability to maintain the confidentiality of the information that they hold. Hence, they understand the importance of encryption and security, and implement the necessary security measures. It is generally worth assuring the public of this point.

Chat

Chat originated as text-based conversation – hence its name. Unlike e-mail, chat is instant, messages you type appear instantly on the computers of other people logged into the chatroom.

More recently, these messages have begun to include sound and images, blurring the line between chat and telephony. Chatrooms generally have a theme, such as a particular hobby or pastime, or they may be run alongside a TV programme so that viewers can discuss the show.

Chat suffers from the same problems as other online activity, including the difficulty of establishing the real identity of people – yet chat is a far more public forum, where you are more likely to meet people for the first time. Some chatrooms have rules of acceptable conduct and are described as ‘moderated’: this means that they are supervised and that the moderator can eject people who break the rules. However, the level of supervision can vary a great deal. In a similar manner to e-mail, chat may seem trivial and ephemeral, but this does not remove the chance that it may be stored and archived.

Wireless Networks

A relatively new development is the rise of wireless networks – most of which use either ‘Bluetooth’ or ‘Wi-Fi’ technology. These wireless systems allow computer networking without wires, so a suitably-equipped laptop computer, partnered with an access point, can surf the web in the garden or access e-mail in the kitchen. Most of these devices can protect their communications with encryption, but are generally sold with the encryption options turned off in order to make set-up easier. The disadvantage of this approach is that many people never activate encryption and it is very easy for anyone with a suitably-equipped computer, who is within range, to gain access to an unencrypted wireless network. Although standard encryption will make the wireless network less vulnerable, a determined and sophisticated attacker can break most of the standard encryption schemes, given enough time.

Mobile Phones

The most immediate risk with mobile phones is that both adults and children can rapidly run up very high bills. Similarly, with expensive new mobile phones there is also the very real risk of theft, and as mobiles bought with a contract are heavily discounted, many users are unaware of the true cost of their phones. In the long-term, the possible health risks of excessive mobile phone usage, although certainly small, may not be negligible.

Spam text messages, similar to spam e-mail, are an increasing irritation. Children especially need to be warned against giving out their personal details to unknown callers, or in response to text messages. Moreover, users should also be aware that with the increasing sophistication of today’s new mobile phones it is likely that mobile phone viruses – along the lines of today’s computer viruses – will soon emerge.

Before You Start

Having presented the potential risks that are applicable to the different uses of ICT by citizens, this Guide will proceed with a demonstration of how to structure and implement a public awareness campaign related to information security. It is crucial to remember that any awareness campaign requires careful planning – whether it is a one-off event or a long-term project involving many different strands. The rest of this Guide provides an introduction to many of the issues that you will need to deal with in order to organise such a campaign.

The Annex to this Guide provides a summary of specific methods that can be employed in awareness-raising campaigns and the issues to consider when using them.

The first issue to deal with is to establish your aims and objectives. It is vital that you spend time at the beginning of the project thinking about your aims, clearly establishing exactly what

you hope to achieve. If you fail to do this you are in danger of adopting an inefficient, random approach in an attempt to hit some of your target audience, some of the time.

There are a number of questions that you need to answer when thinking about your aims and objectives.

- Why are we undertaking this campaign?
- What are the key issues that we wish to address?
- Is there an obvious problem?
- Why are we addressing this problem and not another one?
- Are we the right organisation to be addressing this problem?

When you are thinking about your aims, try not to make assumptions: ask yourself what data – such as surveys, published research – backs up your position. It is vital to try and avoid basing your aims, objectives and strategy on anecdotes and guesswork.

Your objectives result from your aims. But whereas aims are aspirational and hard to measure – such as ‘increase home workers’ awareness of information security’, objectives are more specific, precise, realistic and ideally measurable. For example, an objective related to the previous aim could be ‘to reach 50% of home workers with information about backing up and keeping their operating system up-to-date within a year’.

Addressing whether you are the right organisation to undertake the campaign may be a hard question to answer honestly, but is very important. Ask yourself the following questions.

- Do you have access to your intended audience?
- Do you have the necessary resources?
- Will your audience trust you to tell them about information security?

If the answer to any of these questions is no, you should certainly consider working with a partner organisation.

Partners

Partner organisations can bring a number of benefits to your campaign.

Access to an audience

A partner organisation might already have access to your intended audience. For example, teachers’ associations or teaching unions might assist you in reaching teachers and pupils.

Trust and authority

Your intended audience might hold a partner organisation in higher regard, because of its commitment to independence or recognised experience in dealing with such issues (e.g. consumer organisations).

Expertise

A partner organisation may bring additional expertise through having worked in another area, such as advertising, or reaching audiences through the web.

Resources

A partner organisation may provide additional monetary or human resources to the campaign.

Co-operating with partner organisations assists in providing varied sources of information that can be used as part of a campaign. Such a variety of sources, e.g. independent agencies, leading academics, industry bodies and non-governmental organisations (NGOs), makes it easier for people to distinguish between assumptions and judgements and so allows them to trust the information that is being presented to them.

Inevitably, working in partnership involves compromises between the collaborating organisations, so it is important at the outset to establish the priorities for the campaign and agree on whether all organisations involved can sign up to exactly the same message.

As well as agreeing a common message, you need to consider wider issues of corporate ethos.

- Do your organisations have similar outlooks on other issues outside of raising awareness of information security?
- If your organisations have different views on, for example, censorship of web content, or privacy concerns, how will you manage this?
- How do your wider stakeholders view your partner organisation?

Certain audiences may also react against the inclusion of commercial partners who could be perceived to have their own interests at stake, i.e. promotion of their own products. Examples of partner organisations are:

- makers of antivirus or firewall software;
- computer manufacturers or re-sellers;
- media organisations;
- churches/other religious organisations;
- trade unions; and
- consumer organisations.

Who Are You Talking to? What Is Your Message?

The public consists of a hugely diverse collection of individuals with differing interests, expertise and priorities. These individuals fall into a myriad of overlapping groups that have certain characteristics in common, such as age, sex, the publications they read, their religion, even where they buy their groceries. It is very hard to find issues, images and messages that will have relevance to everyone.

Because of this, it is generally necessary to target a specific group of the public that has similar interests and priorities.

You will have to address three questions about your audience.

What Will They Notice?

You need to capture your audience's attention, and the type of audience you seek to address should determine the method you choose to do this. For example, cinema adverts might be a great way to target young adults, but information on the back of breakfast cereal packets might be a much better way to target parents with young children.

Why Should They Care?

You need to tailor your message to your audience's interests and concerns – grandparents who use e-mail to keep in touch with family members, but never buy anything on the web, may be interested in a message about dealing with spam, but will not be engaged by a message about protecting your credit card number when purchasing online.

What Will They Do?

You need to consider the kind of activities in which your audience might take part. For example, parents may have to arrange for childcare to attend evening events, but if you could run those events alongside a school parents' evening, they will already have solved this problem.

You also need to consider what action you are likely to be able to persuade your audience to take. For example, how much information will inexperienced users need in order to select, install and configure antivirus software or a firewall – should you be suggesting that they ask a more technically experienced friend or acquaintance for help?

As can be seen, your message and your audience are tightly linked, each affects the other. You could begin by identifying a particular risk you want to concentrate on – perhaps your organisation has expertise in viruses; or you could begin by looking at which audiences you have easy access to – for example, do you already have an education programme and expertise in working with teachers?

There are two ways in which to focus your message: either by dealing with a class of risk – for example, threats to privacy; or by focusing on a specific technology – for example, e-mail. When working with an audience with little prior experience of information security, they are more likely to be able to identify and understand a message that says: 'If you are using e-mail you need to consider the following', than a general message about protecting their privacy online.

Sample Messages

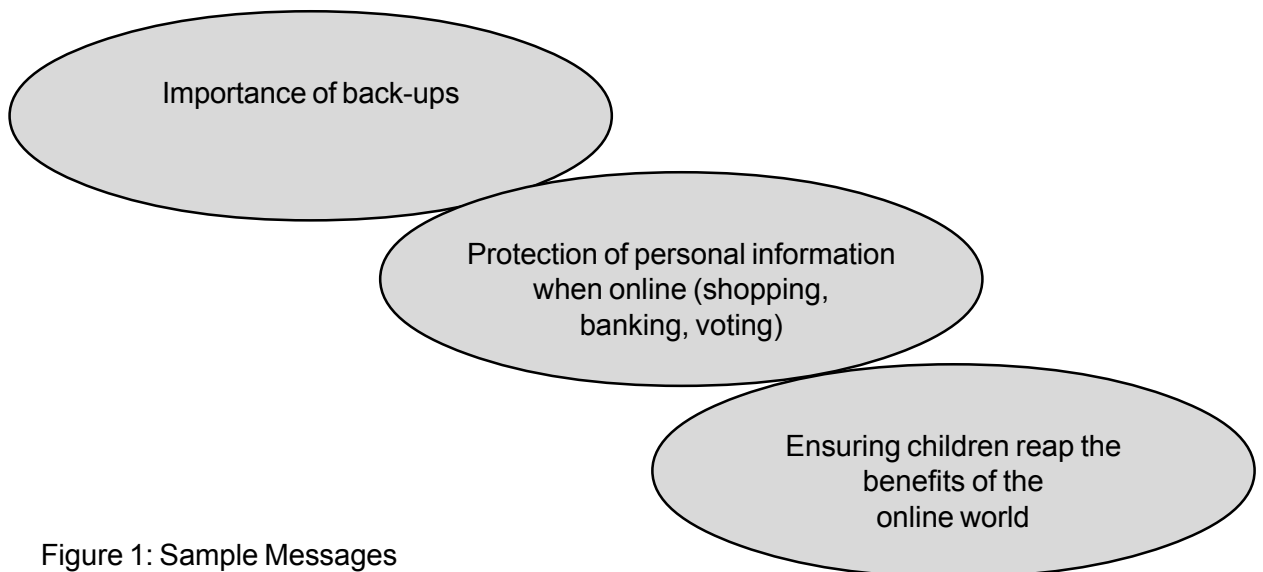


Figure 1: Sample Messages

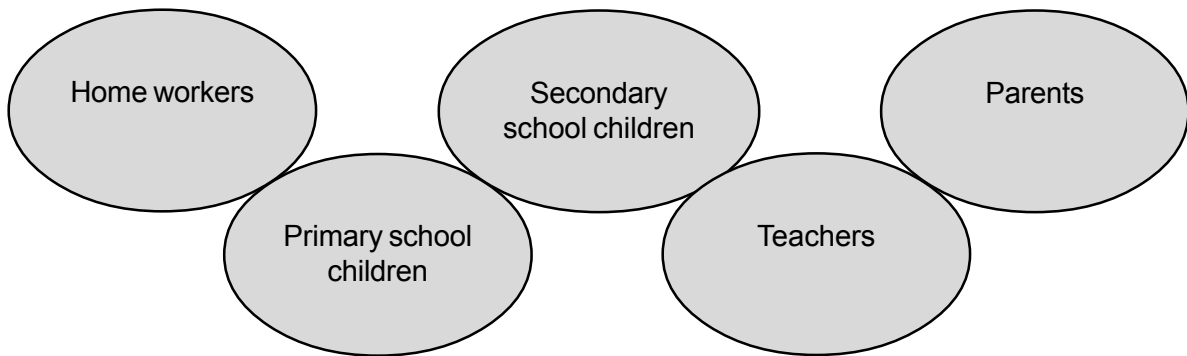


Figure 2: Sample Audiences

Getting the Details Right

Research Your Audience

The only way to come up with an effective message for your audience is to understand them; and to understand them, you must research them. You need to know:

- their level of awareness of information security issues;
- the purposes for which they use ICT;
- the issues that they are concerned about;
- where they get their information at present; and
- what information they would like to receive.

You can use a survey, focus groups or informal discussions to find out such details. The more information you have, the better – although any information is valuable.

Once you have come up with a message for your campaign, it is very important that you test it out on the intended audience. Find some members of your target audience and see what they think of your message and the way in which you intend to deliver it. This testing should also help you to identify likely ways in which your audience may misunderstand your message. You may discover that your audience does not understand the difference between the Internet and the web, or they may assume that all communication across the Internet is point-to-point, in a similar way to a telephone call.

Message Contents

Your message needs to do three things:

- (1) catch your audience's attention;
- (2) alert them to a risk or issue in terms that they can understand; and
- (3) provide them with enough information to address the risk or issue.

The third point above is both important and possibly the hardest to achieve. If you fail to provide your audience with a way to address the risk, your campaign will simply serve to alarm and worry them. For example, if you warn people about the dangers of viruses, you need to provide them with information about how to protect their computers, reviews of antivirus software, or suggestions about where they can find this information. Although referring your audience to another source of information can help to keep your message short and punchy, there is the very real danger that your audience will not be sufficiently interested in your message to refer to this source, and therefore will never see that additional information.

Technical Level of Information

You must bear in mind the technical expertise of your audience. If you recommend that they install Internet filtering software, you might need to think about the following issues.

- Will they know where to acquire it?
- Will they know what to ask for?
- How will they decide which version is best?
- Will they understand how to install the software?

Bear in Mind Competing Messages and Risks

Bear in mind that many different marketing messages will be bombarding your audience. Look at your campaign from your audience's point of view: what will make them notice and listen to your message?

Your audience will also be dealing with many other real world risks and issues – whether they should have a flu vaccination, which car they should buy, what precautions they should take when walking home at night. Information security will be but one risk among many. You need to provide them with compelling reasons as to why they should address an information security risk, rather than one of the other issues that they are currently tackling. One way to achieve this could be to convince them that the information security risk is the most serious of all risks that they face. However, this is unlikely to be the case. Furthermore, exaggerating the risks posed by information security will alarm your audience, making them less likely to take advantage of ICT, and could damage your organisation's credibility.

It would be much better to suggest simple, quick and cheap ways to address your chosen risk, and use this as the justification for dealing with your risk first.

Comparisons with the Real World

If you are dealing with an online risk with which your audience is likely to be unfamiliar, can you compare it to a real world risk of which they have experience? For example, how does the likelihood of online credit card fraud compare to that of normal credit card fraud?

Reaching Your Audience

Can you work through, or with, a group that has easy access to your audience? Such mediators could include libraries, local trade organisations, community centres, computer stores, community colleges and adult education programmes, parent teacher associations, etc.

If you are considering targeting an audience that has little experience of using computers – for example, retired people – it might be more effective to reach them through the people who help them with their computers, possibly their sons and daughters. If you want to reach parents, you may be able to connect with them via a school-based campaign that targets their children.

Inclusiveness

You need to ensure that any initiative or campaign is as inclusive as possible. If you are using role models, make sure that they also represent any minority communities within your audience. In addition, you should find out whether any of the minorities within your audience have special concerns or views with respect to information security or the message that you wish to promote.

Another important group you should consider is the disabled – how will they access your campaign? Are the venues wheelchair accessible? Are the leaflets readable by those with poor

eyesight? Is the website accessible to blind people? If people with learning difficulties or those with low literacy levels are likely to be an important part of your audience, this raises further issues of accessibility.

Finally, there is another aspect of inclusiveness that is more specific to the field of information security. In the case of computing-related issues, do you need to cater for different information technology (IT) systems? Solutions for Microsoft Windows may not apply to Mac operating systems or Linux, and may not even be the same for different versions of the operating system. Excluding users or advocates of one system from your campaign could undermine your credibility or lead to negative publicity.

Engaging Your Audience

Can you use graphic design that is likely to appeal to your audience? If you are targeting children, can you make use of a mascot or cartoon character with which the audience can identify?

Resistance to Spending Money

Will the actions you are suggesting cost your audience money, for example, buying antivirus or web filtering software? If so, they may suspect you of having commercial motives. Have you addressed whether there are any cheaper or free alternatives?

Spreading the Word – Getting Publicity

Getting publicity is a vital part of any awareness-raising campaign: publicity multiplies your impact by increasing the number of people who hear about your message. Getting publicity is a complex business and can depend as much on contacts and networking as your message and its contents. If you can afford it, it pays to get professional advice and expertise.

You need to consider when and where you want publicity: do you want it beforehand, to attract an audience; or during and after the event to increase the campaign's impact by reaching a larger audience? Do you want to reach everyone in a specific geographical area, in which case local media is your target; or everyone in a specific group, for example, teachers, in which case a better target would be specialist magazines for teachers?

When dealing with the media it is very important to remember that their sole purpose does not revolve around spreading your message. Most of the media are trying to attract readers, listeners or viewers and sell their product; even publicly-funded media want high viewing figures or circulation.

Journalists want to write stories that will attract their audience, so you need to consider their priorities when shaping your message. At minimum you need to know who they consider their audience to be. You also need to bear in mind that you cannot control what the media write, perhaps only influence it. Think carefully about your message and how it could be misunderstood or sensationalised, and make sure you include all the relevant caveats, explaining the issues in simple, jargon-free language.

Press Releases

If you do not have contacts with journalists, then press releases are the key to getting news-related publicity. Some of the basic points to bear in mind are as follows.

Relevance

Work out why your story will be relevant to the audience of the publication: if it is a local paper, why is the story particularly relevant to the local community? Ask yourself why your topic is current and newsworthy.

Length

Keep press releases short, one page of A4, one and a half-spaced, at most.

Make it a People Story

The media are far keener on stories that are about people, than stories about technology. Try and find a human face for your story.

Quotes

If possible, include an interesting quote that the media can use that encapsulates part (or all) of your message.

Contact Information

Do not forget to include your contact information and details of where the journalist can find more information (such as a website). Remember that generally, journalists will be working to very tight deadlines, so give a telephone number where they can contact you.

Send to a Named Journalist

If possible, send your press release to a named journalist, or at least a specific editor. It is often worth contacting them in advance to see if they are likely to be interested in your story. If you do this, make sure you can sum up what your story is and why it is interesting to their audience in 30 seconds or less.

Interviews

Preparing for interviews is extremely important – especially for broadcast media, where there is less chance to correct what you say. Select a few key messages (no more than three for a short interview) and practise being questioned by a friend or colleague. Try to avoid reciting verbatim pre-written answers, as they can come across poorly and there is no guarantee that you will be asked the right question. You should also consider who is the most appropriate spokesperson for the interview's audience; if it is a television interview, think carefully about what clothes to wear, in line with the audience you are aiming to engage.

Other Places to Get Coverage

As well as the news sections of the media, many newspapers (and local radio and TV channels) have 'What's On' sections. Find out which media outlets your intended audience reads and get

in touch with the editors of these sections. You will probably need a different press release for this, particularly one that emphasises why their audience will be interested in your event and what they will get out of it.

Facilities for the Press

As well as publicity before the event, you should think about whether you want the press to cover the event itself. If so, you will need to provide facilities for journalists. They will want access to telephone lines, a space to carry out interviews and sockets to plug in their laptops. Also, you may want to consider bringing in a professional photographer to take photos of the event that can then be used by the press, including those media channels that did not attend the event.

Checking it Worked

Although this is the last section of the Guide, evaluation is something that you should be thinking about from the beginning of a campaign. Formal evaluations should be rigorous and independent, but less detailed evaluations can also provide valuable information on how to improve your campaign. An evaluation can be broken down into two parts: a quantitative aspect, such as counting audience attendance; and a qualitative aspect, to find out your audience's opinions on your campaign, possibly interviewing select members of the audience before and after an event in order to examine changes in knowledge or attitudes.

There are three basic methods of exploring the views of participants, and a fourth that can be used for very large-scale campaigns:

Focus Groups

- These bring together small groups of 8–12 participants to discuss their experiences of the event, leaflet or education pack.
- They are ideal for exploring issues in depth and focusing on 'how' and 'why' questions.
- Focus groups are run by a neutral facilitator whose role is to probe participants' views, summarise the feelings of the group and poll opinion within the group.
- A 'topic guide' of wide and open questions forms the agenda for the discussion, which is generally recorded and transcribed.
- Analysis of focus group output is subjective, and because of the small number of participants the output is not statistically representative.
- They can be a good way to explore the kinds of issues should be covered in questionnaires and the range of experiences and opinions that an audience may have.
- Focus groups last for a couple of hours and it is generally expected that refreshments and a financial inducement will be provided to participants.

Interviews

- These are the middle ground between focus groups and questionnaires, requiring fewer resources than focus groups, but providing more depth and detail than questionnaires.

- Because the interviewer talks directly to the participant, they are likely to obtain more information than would be written on a questionnaire, and the personal approach should help to increase the response rate.
- You can carry out interviews either face-to-face or over the telephone, but eitherway it is often helpful to record interviews in order to ensure that you have an accurate record of the interviewees' responses.
- You should always ask the interviewee's permission for recording and be willing to take notes if they refuse.
- You may want to interview people both before and after they encounter your campaign, in order to find out the impact that it has had.

Questionnaires

- These are a good way to collect information from many participants, although only simple information can be collected, as people are only willing to spend a short time filling in a questionnaire.
- Response rate – i.e. the number that are filled in and returned – is often a problem with questionnaires. If your response rate is low, you cannot know that the questionnaires you received represent the views of the entire audience, as people who hated or loved an event might be more likely to fill in a questionnaire.
- One way to improve response rate is to provide some small incentive for questionnaire completion, or to set aside time in the programme of an event specifically for questionnaire completion. One possible incentive is entry into a prize draw; however, this raises issues of how confidentiality of feedback can be ensured.
- Always provide the opportunity for respondents to include other comments they may have – they may have a great idea for a way in which to improve your project – so give them space to write it down.

Omnibus Surveys

- Some market research organisations carry out regular omnibus surveys with particular audiences, for example, every six months the research organisation may put together a panel of several thousand schoolchildren and administer a questionnaire to them.
- These questions come from a number of different organisations. Buying such questions can be a much cheaper way to explore the attitudes of your audience, and to see whether your campaign has had an impact, rather than commissioning your own survey.

Annex: Methods of Communication

This section covers many of the specific methods that you might use in an awareness campaign – posters, websites, workshops, etc. It provides an introduction to the main advantages and disadvantages of each approach and a summary of key issues that need to be considered when using each approach.

	Advantages	Disadvantages	Issues
Websites <ul style="list-style-type: none"> • Very useful as a source of information for the technically literate 	<ul style="list-style-type: none"> • Can be updated to reflect changes in situation • Can present content for multiple audiences • Can easily link to other information 	<ul style="list-style-type: none"> • May not reach a technologically naïve audience • Needs constant maintenance 	<ul style="list-style-type: none"> • Need to make it accessible and easy to use • Do not over design – design for the intended audience • Need to make sure links point to what you say they do and that they do not break
School-based campaigns	<ul style="list-style-type: none"> • Good way to reach large numbers of children • There are established routes to reach education audiences 	<ul style="list-style-type: none"> • Time in school is already at a premium and curricula are often overcrowded • Teachers may not have expertise to deliver message • Computing facilities may not allow some activities – e.g. practice in installing antivirus software 	<ul style="list-style-type: none"> • Need to include curriculum relevance, and teachers notes that give background information • Need summary of why a teacher should use the resource that can be read in 30 seconds • Need methods of delivery to teachers • It may be more effective to work indirectly, by lobbying for changes in curricula in order to increase emphasis on information security
Talks <ul style="list-style-type: none"> • Similar to workshops but less interactive 	<ul style="list-style-type: none"> • Can reach very wide range of audiences by careful selection of venues and topics • Potential to reach a large audience with only one speaker 	<ul style="list-style-type: none"> • Your intended audience may not attend 	<ul style="list-style-type: none"> • Can you find a venue that your target audience already uses, so they will feel comfortable? • Start with familiar subjects and then move into the less familiar information regarding information security • Use visual aids, make talks varied and interesting • Provide written copies of any information (for example, URLs) you want your audience to remember • Use simple graphs, not tables or figures
Workshops <ul style="list-style-type: none"> • More interactive than talks, for a smaller audience 	<ul style="list-style-type: none"> • If people have the opportunity to try things out, they are more likely to remember them 	<ul style="list-style-type: none"> • Labour intensive, you will need many demonstrators/explainers to work with the audience 	<ul style="list-style-type: none"> • Involving celebrities is a way to attract attention and increase attendance at events and workshops
Competitions and quizzes <ul style="list-style-type: none"> • Either large-scale competitions or small-scale quizzes as part of a large campaign 	<ul style="list-style-type: none"> • Can reach wide audience • Engages audience in thinking about the issue • Relatively low administrative costs 	<ul style="list-style-type: none"> • Will a quiz allow you to provide enough information? 	<ul style="list-style-type: none"> • How will you publicise the competition and get entrants?

	Advantages	Disadvantages	Issues
Screensavers <ul style="list-style-type: none"> • Screensavers with information security messages 	<ul style="list-style-type: none"> • Puts information on the computer so users are likely to see it 	<ul style="list-style-type: none"> • Requires development • Inexperienced users may be unable to install them • Does not reach those without computers 	<ul style="list-style-type: none"> • Will you provide different versions for each computer operating system?
Grant schemes	<ul style="list-style-type: none"> • Takes advantage of creativity of individuals and other organisations • Can be shaped to local conditions • Low administrative burden 	<ul style="list-style-type: none"> • Issues of quality control • Reputational risk of being associated with grant projects that go wrong, or that promote incorrect messages 	<ul style="list-style-type: none"> • How will you publicise the scheme to likely applicants? • How will you judge the applications? • What support will you provide for grant recipients?
Leaflets <ul style="list-style-type: none"> • 	<ul style="list-style-type: none"> • Can provide a lot of information • Relatively cheap to produce 	<ul style="list-style-type: none"> • Need to organise distribution channels so your leaflets get to the people who need them • Leaflets need to catch your audience's attention – without causing alarm 	<ul style="list-style-type: none"> • Could you distribute leaflets where people are buying the technology in which you are interested? But how many people read the information that comes with their new computer? • Can you find somewhere that people will pick up and read leaflets? • All printed material benefits from attractive visual design, but the design should not make it hard to read
Posters, trinkets and giveaways <ul style="list-style-type: none"> • Posters, pens, keyrings, post-it notes, bookmarks, mugs, mousemats, etc 	<ul style="list-style-type: none"> • Relatively cheap to produce • Most people like 'something they can take with them' 	<ul style="list-style-type: none"> • Needs distribution channel • The message must be very simple. Re: posters – your audience will have to remember slogans, catchphrases or mascots. If you use posters to publicise your website, is the URL simple enough to remember? 	<ul style="list-style-type: none"> • What types of items are your audience likely to pick up, keep and use?



www.eaware.org

RAND Europe
(Project coordinator)

www.randeurope.org



www.clusit.it



www.eltrun.aueb.gr

intellect

www.intellectuk.org



www.ecp.nl



escert.upc.es



www.praxis.ee



www.timekontor.de



www.danishtechnology.dk

INFOLAB

jango@pg.gda.pl