Security Awareness for Children

Clara Brady

Technical Report
RHUL–MA–2010–05
31st March 2010

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England

http://www.rhul.ac.uk/mathematics/techreports

Security Awareness for Children

Clara Brady

Supervisor:

Chris Mitchell

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledge all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature Date

Table of contents

Abstract

The Internet plays an increasingly larger role in the everyday lives of our children [LS-09d]. As a learning and communication tool, it offers them a wide range of opportunities [SM-08]. It is an invaluable source of knowledge and encourages creativity and imagination. Research has shown that three quarters of European children are online availing themselves of these opportunities [LS-09d]. Unfortunately, use of the Internet has negative consequences: risks are encountered. These risks range from exposure to inappropriate content, undesirable contact from strangers, and even cyberbullying. Children may not have the necessary skills or knowledge to manage these online risks [BT-08]. So what can we do to protect them and ensure that they enjoy a safer, online experience?

Eliminating online risk is an impossible task. Efforts in the past have focused on reducing children's exposure to risk by controlling their access. Parental controls and monitoring, age verification solutions, walled-garden online environments and child-only social networking sites are some of the ways this can be achieved. However research has shown [N-09] that children can circumvent these measures. It also limits their opportunities and leaves children whose parents are not tech-savvy still at risk. It is clear that a more effective solution is needed. We can empower our children with the necessary knowledge and skills they need to stay safe online [BT-08]. We can raise their awareness of the risks they face and educate them about the safety and security issues they may encounter.

An Information Security Awareness programme designed specifically for children will achieve this goal. It will encourage children to adopt safe computing skills and will promote good security practice. It will aim to make children aware not only of the risks they face, but also of the countermeasures they can utilise to protect themselves.

This paper considers the need for an Information Security Awareness programme for children. It identifies the categories of risk children face online, discusses the results of a survey investigating children's online activities and outlines the objectives of an awareness programme for children. By implementing such a programme, the author believes that we can allow our children to reap the full benefits of the Internet and enjoy a safer online experience.

Chapter 1

Introduction

1.1 Background

Research has shown that three quarters of European children are online availing themselves of the opportunities afforded by the Internet [LS-09d]. It plays an increasingly larger role in the everyday lives of our children. As a learning and communication tool it offers a wide range of opportunities for people of all ages [SM-08]. It is an invaluable source of knowledge and encourages creativity and imagination. Unfortunately, availing of these opportunities has negative consequences: risks are encountered.

As a human race we have been dealing with risk since the beginning of time. Risks surround us in all areas of life: at school, at home, in the city and in the countryside. With the advent of the Internet came an additional area of life where we encounter risk; risk in the digital world. This new area of risk has given rise to widespread discussion, debate and anxiety, in particular, online risk for children. Although parents are quite confident in their ability to guide children to become competent risk managers in other areas of life, some parents feel powerless when it comes to helping their children manage this new area of online risk. This feeling of powerlessness may be due to the generational digital divide that exists between parents and children. Parents feel that they lack the knowledge, skills and understanding of this new technology that is required to teach their children how to stay safe online. This results in a role reversal whereby children are more skilled in their use of technologies than their parents. Many parents are uncomfortable with this role reversal and thus become apprehensive about their children's use of the Internet [BT-08 Ch. 1 pg 22-25].

Use of the Internet exposes children to a wide variety of risks. Children may not have the skills or the knowledge to manage these risks. Efforts in the past to protect children from these risks have focused on controlling children's access. However controlling access, limits their opportunities [BT-08]. Therefore in order to allow children benefit from the opportunities the Internet affords and to protect them from the risks it presents, it is vital to

empower them with the necessary knowledge and skills to stay safe online. It is vital to raise their awareness of the safety and security issues they may face and to increase their resilience to these risks.

Empirical research on the efficiency of training, campaigns and rewards in other fields suggest that approaching safety and security awareness in this way will have the potential of improving children's awareness. Training has proven beneficial in AIDS prevention [OD-89], awareness campaigns have proven successful in road safety [DA-04] and rewards have been considered as effective in motivating humans to change attitudes and behaviours for a long time [FL-59]. Therefore one can conclude that appropriate education and awareness programmes will be effective in increasing cyber security awareness in order to protect children while online. Schools are a universal point of contact through which children can be reached. Thus it is vital that appropriate education programs are put in place in schools to enable them to become safer, wiser and more responsible Internet users.

1.2 Project Objectives

In the past the cyber security was a concern for computing professionals and government agencies only. With the popularity of the Internet, it is now a shared responsibility of adults and children alike. By teaching children effective age-appropriate cyber security skills from the start they will develop positive security habits from an early age and will grow up to become responsible, security conscious cyber citizens.

> *"Reaching school children, many of whom are the current technology experts in their homes, enhances a responsible culture for now and in the future."*
>
> John Colley (ISC)[2]

As a primary school teacher and an information security professional, the author of this paper realises the importance of teaching children these skill and this project aims to utilise her knowledge from both professions to create guidelines to develop a cyber security awareness programme for children.

The objectives that this project sets out to achieve are;

1. To review the existing research on the issues and dangers children face on the Internet.

2. To examine children's online habits and the nature of their access.
3. To identify the risks children may be exposed to as a result of online activity.
4. To identify the existing cyber security resources available.
5. To examine existing security awareness approaches.
6. To create guidelines to develop a cyber security awareness programme for children

1.3 Methods used

A literature review was conducted to collate all the relevant research that has been carried out to date. This was analysed to ascertain the concerns and issues that have been raised regarding children and the Internet. The author chose two studies to focus on; The European Commission's *Safer Internet for Children Qualitative Study* and the National Centre for Technology in Education's *2008 Survey of Children's Use of the Internet in Ireland*. The former paper was chosen as the target audience was closest to the target audience the author wants to focus on and the latter because it demonstrates many significant changes in children's Internet use.

The age range of the focus group for the cyber awareness programme is ten to twelve years. To date no research focuses solely on this group. The author distributed self administered surveys to four primary schools in Ireland. There were three different surveys each designed for a different target audience; primary school pupils aged between 10 and 12, parents of these pupils and teachers. This survey completed by 202 Irish children aimed to gather evidence on these children's Internet habits; frequency of access, location of access, surfing habits and their opinion of Internet. Parents were surveyed to gain a general understanding of their attitudes and habits regarding their child's Internet access and to identify the extent of their knowledge of some technological safety features. A third survey was designed to obtain evidence regarding teacher's use of the Internet with children and to ascertain their knowledge of existing child e-safety initiatives.

Chapter 2

Risks on the Internet for children

2.1 Introduction

This chapter aims to analyse the existing research on the issues and dangers children face on the Internet. Section 2.2 will present a classification of such risks with a description of each type. Following this section 2.3 analyses the nature of children's access habits and their online interests. Using the information, the author presents her opinions on the risks children face according to the activities they partake in. Finally section 2.4 uses a risk management approach to identify a solution to enable children deal effectively with these risks.

2.2 Risks for children using the Internet

There are a number of online risks for children due to the anonymous, ubiquitous nature of the Internet and the degree of communication it offers [BT-08].

The EU Kids Online network [HU-07, Ch. 1, pg 8-10] classifies online risks to children according to three categories – content, contact and conduct. Content risks refer to risks in which the child is exposed to mass-distributed content. Contact risks refer to risks which may occur when the child is engaged in communication. Conduct risks relate to risks in which the child may be the initiator or actor of content or contact risks.

2.2.1 Content risks

- Age inappropriate content - The Internet hosts an abundance of information for its wide variety of users. This information is easily accessible to all users and can be spread quickly and freely to users all over the world. However some of this content is not appropriate for all ages and children may be exposed to it by actively searching for it themselves or by coincidence. A study [FA-07] of 40 UK websites

that are used most frequently by children revealed that "*less than one-third of these sites are actually designed for children.*" This therefore increases the likelihood of content risk. There is a variety of information on the Internet that can be classified as inappropriate for children and exposure to this may even have negative effects on a child. Age inappropriate content includes illegal content such as child pornography or racist content, through to harmful content which can range from hateful content to violent material. Extensive work has already been carried out by numerous bodies and governmental organisations (Office for Internet Safety, Ireland; Child Exploitation & Online Protection Centre, UK; Insafe, EU) to deal with illegal content online. However, due to the emergence of Web 2.0 which allows users upload content, it continues to be an on-going problem thus posing a risk for children.

- Incorrect content – Due to a number of Web 2.0 applications, users can now upload their own content to the Internet. This content can be uploaded to blogs, wikis, social networking sites and chat rooms. This material is not subject to scrutiny by experts to check its correctness or otherwise. There is no specific place in which to enforce "editorial control" on this user-generated content [BT-08]. Due to this it is very difficult to control the content that is published on the Internet. This enables children to obtain incorrect or biased content when they surf the net. Young inexperienced Internet users are vulnerable to this as they do not have the media skills to deal effectively with this risk and may take the information at face value.
- Commercial content – The study, [FA-07], also revealed that 95% of the 40 websites children most commonly used most often contain some form of commercial content. This type of content ranges from advertising the sale of goods and services, marketing, spam and sponsorship. This poses a risk to children as they may not have developed the media literacy skills to deal effectively with exposure to this material.

2.2.2 Contact risks

- Undesired contact - With the increase in use of social networking sites and instant messaging services, children are potentially at a greater risk of receiving unwanted

and inappropriate contact from strangers and cyber bullies. It is known [C-02] that one medium that paedophiles use to make contact with children is the Internet. As children are now becoming more frequent users of chat rooms and instant messaging services, they may be at a greater risk of being groomed.

> "*Cyberbullying involves the use of information and communication technologies such as e-mail, cell phone and pager text messages, instant messaging (IM), defamatory personal Web sites, and defamatory online personal polling Web sites, to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others."*
>
> Bill Belsey

Cyberbullying is bullying that is carried out using Information & Communication Technology, particularly mobile phones and the Internet. According to research children are using Information & Communication Technology more frequently thus putting themselves more at risk of being victims of cyber bullying.

- Disclosing of personal information –Young people and children are increasingly putting personal information on the Internet through chat rooms and social networking sites [N-09a]. Two thirds of the sites used most frequently by UK children ask for personal information to join clubs, sell products, enter competitions and create online identities [FA-07].Children may be oblivious to the dangers associated with disclosing sensitive, private information online and unaware of privacy rights. Children may not understand the need to check that the information they provide will be managed properly by the site. Being unaware of this threat can lead to the wide range of risks ranging from phishing attacks to being recipients of inappropriate advertising or marketing therefore increasing their vulnerability to undesired contact.

2.2.3 Conduct risks

- Bullying or harassing other children
- Creating/uploading incorrect or harmful material

- Illegal downloads

2.2.4. Security risks

There are numerous security risks for all users of the Internet. The author believes that these risks also apply to children. The activities that children partake in online will determine which of these general user risks children are susceptible to. These security risks range from viruses, spyware, spam, to identity theft, disclosure of personal information and phishing.

2.3 Children interests and nature of Internet usage

Identifying how children are using the Internet, the activities they partake in online and the nature of the child's Internet access can determine the extent to which children may face information security risks. The activities they partake in will determine the type of risk they are exposed to and the nature of their access will have a bearing on their vulnerability to the risk.

2.3.1 Research to date

Much research has been carried out on the topic of children and the Internet [N-09a, EC-07, N-03a, BT-08]. The EU Kids Online Network compiled a report, [LS-09b], identifying the research carried out on children and young people's access to and use of the Internet and online technologies across Europe. According to this report [LS-09b] the most researched topics are online usage followed by access, interests and activities. Other areas of research are based on children's online skills, social networking online, playing online games, the effects on children of going online, concerns and frustrations of children and children's identity play. Very little research has been carried out in the area of civic and political participations, interpreting online content, seeking advice online and strategies for finding things.

2.3.2 What are children doing online?

The European Commission's Safer Internet for Children Qualitative Study [EC-07] which was carried out in 29 countries in Europe revealed that the Internet is used by children for two main reasons; online games and looking for information on subjects they are interested in which includes browsing for fun. It also revealed that looking for information for homework, communicating, downloading music and sending and receiving emails are also frequent activities that children partake in.

The National Centre for Technology in Education (NCTE) based in Ireland has carried out three similar studies in 2003, 2006 and 2008 investigating children's use of the Internet. The 2008 Survey of Children's Use of the Internet in Ireland [N-09a] reported that the most popular activities on the Internet that children partake in are playing games (60%), downloading music (51%), using social websites (48%), doing homework (43%), getting information not related to schoolwork (38%), sending and receiving emails (36%), using instant messaging (36%) and chatting in chat rooms (18%). It also noted that there had been a significant increase in certain activities including the use of instant messaging and the number of children providing personal information. The NCTE's Survey of Children's Use of the Internet in Ireland [N-09a] also revealed that social networking has become a daily activity for most children, particularly teenagers.

In the study carried out by this author, it was found that the most common activities that children declared they use the Internet for are playing games (77.95%), looking up information (40%), browsing for fun (36.92%), downloading (32.82%), email (29.23%), social networks (22.56%), msn (13.85%) and making new friends (9.74%).

2.3.3 The nature of Internet usage

While examining the area of online risk, it is also important to assess the nature of children's Internet usage as this will influence a child's vulnerability to these risks.

a) Increase in access from home

A major change emerging in a number of studies is that the number of children accessing the Internet from their own homes is increasing year by year [N-09a, EC-07]. In the study carried out by this author, it was found that the most common location of access to the

Internet was at home (88.72%). Studies have also shown that children who have access to the Internet at home use it on a more frequent basis. [N-09a]

> *"95% of those with access to a computer at home stated that they also have an Internet connection at home, an increase from 90% in 2006 and 80% in 2003."*
>
> *"44% of those who used the Internet at home use it every day or almost every day, an increase of 20% since 2006."* [N-09a]

This increase in home access may be due to the fact that because we live in a culture increasing with risk, children are more restricted to playing indoors and in order to entertain them parents are providing them with a media rich environment [LS-09c, Ch. 1 pg 14]

b) Children are accessing the Internet from a younger age

There is also evidence that children are accessing Internet from a younger age [N-09a] and the notion has been proposed that this trend will continue with the possibility of children starting to use the Internet when they start walking [FO-09].

> *"Children of primary school age and younger are increasingly gaining access to the Internet."* [LS-09a]
>
> *"In 2003 most children were starting to use the Internet between the ages of 9 and 10. In 2006 most children started to use the Internet at age 8. In 2008….more than a third were 7 or younger when they first used the Internet."* [N-09a]

c) Learning through self-discovery

Children reveal that they learn to use the Internet mainly by themselves with some input from older siblings or parents at the beginning to teach them the basics. Overall the majority of children say they learn to use the Internet through a process of self-discovery [EC-07]. In the study carried out by this author similar results were found with almost half of the sample population declaring that they learned to use the Internet by themselves (43.59%). Parent/guardian was the next most common source for learning to use the Internet (33.33%)

followed by siblings (10.77%). Only 4.62% (n=9) declared that they learned to use the Internet from their teacher.

d) Location of computer

There is evidence [N-06] that there is a decrease in the number of children who access the Internet in a public room at home. There is also evidence [HU-07] that due to a number of social changes, there is an increase in 'bedroom culture' with children spending more time at home in their bedrooms than in public spaces. As Internet mobility becomes widespread it is likely that the number of children with access to the Internet in their bedrooms will increase.

Consequences

As the number of children accessing the Internet from home has increased this may increase the frequency of children's use of the Internet which in turn may increase their exposure to online risks. The more frequently a child uses the Internet the more likely it is that they will encounter risk. The age of the child encountering the risk will also have a bearing on the impact of the risk on the child. Considering the fact that children are accessing the Internet at a younger age it is more likely that they will be more vulnerable to certain risks as they will be less likely to have the skills and ability to deal with the variety of online risks.

The way children learn to use the Internet will have an effect on the likelihood of developing good Internet habits. As the majority of children are learning how to use the Internet through a process of self-discovery, it is more unlikely that they will develop good Internet habits than if they were learning from a proficient user.

The location of the computer may determine the degree of a child's risky online behaviour as children tend to behave better if they are being watched by parents. With the decrease in the number of home computers being located in public rooms, it makes it more difficult for parents to monitor child Internet use thus leading to an increased likelihood that children will partake in risky online behaviour.

2.3.4 Comparison of risks, activities and nature of Internet usage

After identifying the online risks children are exposed to, the activities they partake in online and the nature of the child's Internet access, Table A, indicates the relationship between each of these elements. The activities they partake in will determine the type of risk they are exposed to and the nature of their access will have a bearing on their vulnerability to the risk.

2.4 Risk management

The wide range of risks outlined in Section 2.2 provides parents, teachers and policy makers with a difficult task of trying to help children manage these risks. Although children are perceived as tech-savvy users in comparison with their parents, when it comes to online risks, they are perceived as vulnerable to the harmful content and contacts that can be accessed through the Internet [SE-08].

It is clearly evident that creating a risk-free online environment for children is an impossible task. By using a risk management approach a solution to help children manage these online risks and to help parents become more confident at safeguarding their children against these risks can be found.

Risk management is the process of reducing risks to an acceptable level. There are four options for managing risk; transfer, accept, avoid, control. Risk transfer is defined as *"sharing with another party the burden of loss, or benefit of gain, for a risk"* [LN-09]. Risk acceptance is defined as the "decision to accept a risk" [LN-09]. Neither of these methods are applicable in managing online risk for children.

Risk avoidance as defined is *"the decision not to be involved in, or action to withdraw from a risk situation"* [LN-09]. This infers that we would prevent children from accessing the Internet. However this method for managing online risk is not viable. Protecting children by preventing online use would prevent children from benefiting from the numerous online

opportunities that the Internet affords. As the opportunities that the Internet affords are intricately linked with online risks this methods for managing risks is not feasible. Avoiding risk is also a task that many educators and psychologists would not wish to be realised as they appreciate the need for a child to deal with risk in order to reach their full potential. Risk is vitally important for a child's development. Therefore an environment where the child is completely protected from all risks should not be created.

Risk reduction is "*the action taken to lessen the probability, negative consequences, or both, associated with risk*" [LN-09]. This can be achieved through prevention, detection and response strategies. It is this method that has been most frequently used to help children manage risk online. Typically their exposure to risks has been reduced using technical measures. This usually results in limiting children's access to the Internet or by controlling their online activity through parental controls and monitoring, age verification solutions, walled-garden online environments and child-only social networking sites. However these solutions while they can be effective to a certain degree are not satisfactory for a number of reasons. Research has shown [N-09a] that children can circumvent these measures. It also limits their opportunities and leaves children whose parents are not tech-savvy still at risk. It is clear a more effective solution is needed.

In the offline world risks are managed for children by decreasing supervision and monitoring appropriately as the child increases in their ability to recognise and cope with risks. We can also approach online risks in this way. "Children should be gradually introduced to more sociable online environments to prepare them for a networked adulthood" [LN-09].

A more effective approach however is to empower our children with the necessary skills and knowledge they need to stay safe online. We can raise their awareness of the risks they face and educate them about the safety and security issues they may encounter. A Security Awareness programme designed specifically for children will achieve this goal. It will encourage children to adopt safe computing skills and will promote good security practice. It will aim to make children aware not only of the risks they face but of the countermeasures they can utilise to protect themselves. By empowering children with this knowledge, we can ensure that they will reap the full benefits of the Internet and enjoy a safer online experience.

2.5 Conclusion

This chapter analysed the existing research on the issues and dangers children face on the Internet. A classification of such risks with a description of each type was presented and the nature of children's access habits and their online interests outlined. A risk management approach was used to identify a solution to enable children deal effectively with the risks they face online. The author concluded that the most effective approach in order to allow children reap the full benefits of the Internet and enjoy a safer online experience, is to implement a security awareness programme. The programme will teach them to become responsible Internet users and provide them with the skills they will need to deal with the risks they may encounter while surfing the web.

Chapter 3

Security Awareness

3.1 Introduction

In Chapter Two, the risks related to children using the Internet were explored. A conclusion was drawn that in order to protect children from these risks, a security awareness programme for children is required. This chapter examines security awareness and what it means in terms of children. Section 3.2 introduces a definition of security awareness and discusses a number of related issues. Section 3.3 discusses the development of security awareness programmes and introduces some methodologies which are currently in use. Security awareness is then examined in terms of children in Section 3.4 and the development of a programme for children is presented in section 3.5.

3.2 Security Awareness

3.2.1 Definitions and concepts

According to the **Oxford English Dictionary [SJ-89],** awareness is

> *"The quality or state of being aware; consciousness"*

and aware is defined as

> *"Informed, cognizant, conscious, sensible. To be aware; to have cognizance, to know."*

One could conclude from this that the term security awareness refers to knowing about security. However the concept is much stronger than this. Security awareness is defined by the **Information Security Forum's Standard of Good Practice [ISF-07]** as

"*the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organisation and their individual security responsibilities, and acts accordingly.*"

This infers that the term security awareness does not only refer to knowing about security but also to act on this knowledge.

In order to raise information security awareness, a security awareness programme must be implemented [E-08]. A programme is defined in [SJ-89], as

"a plan or scheme of any intended proceedings; an outline or abstract of something to be done (whether in writing or not); Also a planned series of activities or events.."

A security awareness programme is defined in [ISF-07] as a

"continuous undertaking aimed at building and sustaining a security-positive environment."

Thus it can be concluded that a security awareness programme is a planned series of events and activities that occur on a continuous basis to create and maintain a pro-active security setting.

In their **Effective Security Awareness: Technical Report**, the **Information Security Forum [ISF-02]** state that effective security awareness can be accomplished through

"an ongoing process of learning that is meaningful to recipients, and delivers measurable benefits to the organisation from lasting behavioural change."

The **National Institute and Standards Technology (NIST**) paper, **Building an Information Technology Security Awareness Program [NI-03]**, defines an effective security awareness programme as one that

"*explains proper rules of behaviour for the use of agency IT systems and information."*

Thus an effective security awareness programme must be a continuous procedure, which is beneficial to the organisation. It must enlighten users of appropriate behaviour and actions in such a way that they will understand the significance of security for them.

3.2.2 Components

A number of papers namely, ***"The new users' guide: How to Raise Information Security Awareness"*** **[E-08], "Building an Information Technology Security Awareness Program" [NI-03]** and ***"Effective Security Awareness: Technical Report"*** **[ISF-02]** define the components of a security awareness programme as awareness, training and education. The relationship between these components is shown in Figure 3.1.

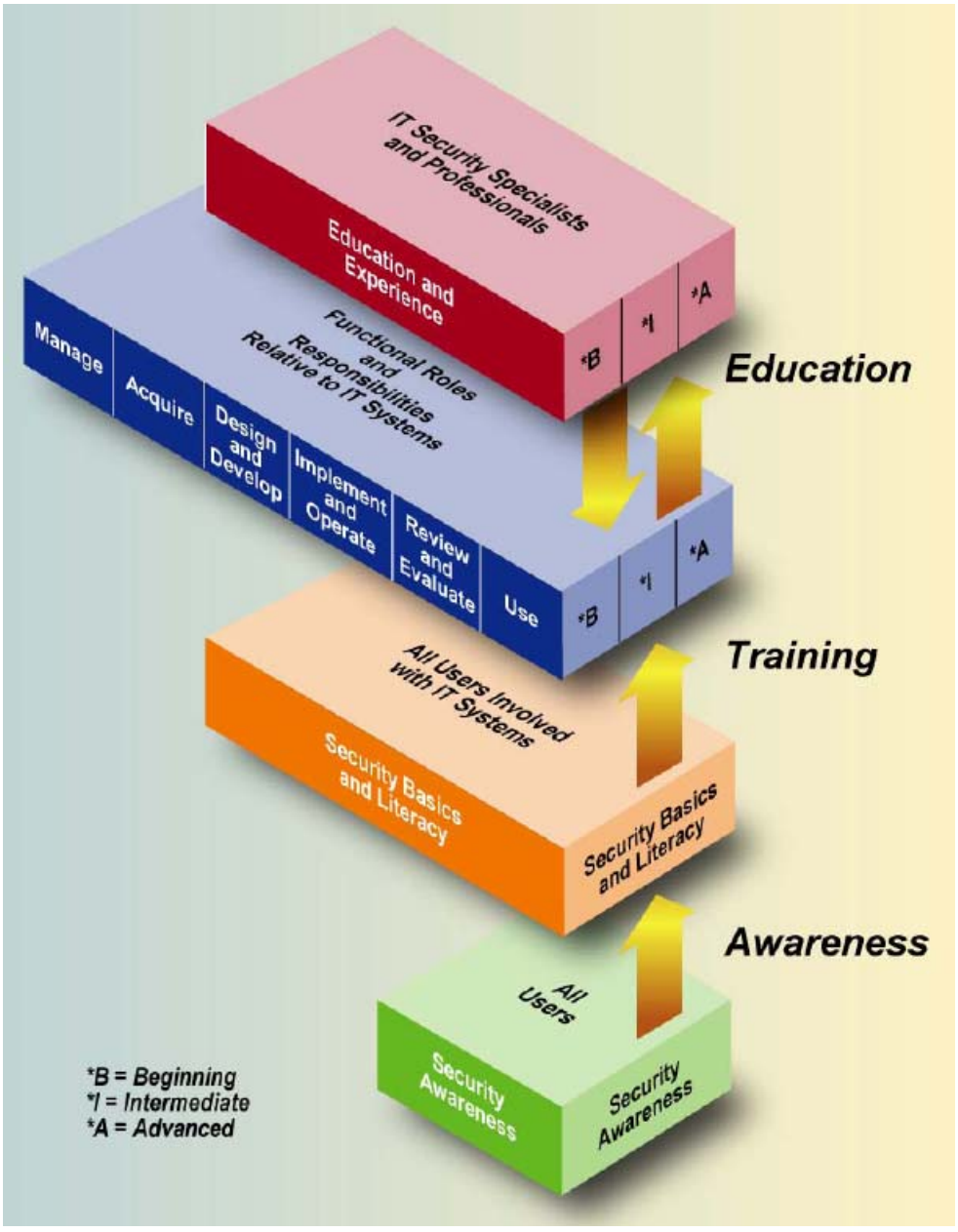

Figure 3.1 The IT Security Learning Continuum

[NI-03]

This diagram represents learning as a continuum consisting of three levels; awareness, training and education.

> *"Learning begins with awareness, builds to training and evolves into education."* [NI-03]

The intention of awareness activities as defined in [NI-98] is

> *"to allow individuals to recognise IT security concerns and respond accordingly."*

Training is defined as the component that

> *"strives to produce relevant and needed security skills and competencies."* [NI-98]

while education brings all the competencies and skills together

> *"as one common body of knowledge to produce IT security specialists and professionals capable of vision and pro-active response."* [NI-98]

Maconachy's psycho-neuronal model as described in **A Systemic-Holistic Approach to Academic Programmes in IT Security [YL-96]**, an educational framework for IT security, is also based on this learning continuum. The goal of Maconachy's psycho-neuronal model of learning is to implant the notion of security into each student. According to this model, awareness involves stimulation, focus, attention, decision and assimilation. Training consists of active knowledge seeking and use of the long term memory while education requires internalisation and accommodation.

> *"Stimulation wakes up the learner, focus makes her delimit the problem from its environment, attention reinforces the problem, decision makes her intentionally remember the problem and assimilation makes her understand the whole problem.*
>
> *Learning causes the learner to actively seek knowledge and remember it while education assists internalisation and accommodation of the principles"*
>
> [LY-96, Ch 5 pg 147-148].

3.2.3 Standards

ISO/IEC 27001:2005 [ISO-05/1] is an international standard which outlines the requirements of an Information Security Management System. One of these requirements is the implementation of Information Security Training and Awareness Programmes [ISO-05, clause 5.2.2]. It states that the organisation must ensure that

> *"all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives."*

ISO/IEC 27002:2005 [ISO-05/2] is an international standard that defines a code of practice for Information Security Management. It provides guidelines on 133 security controls that can be implemented to match the requirements of ISO/IEC 27001/2005. Clause 8.2.2 states that

> *"All employees of the organisation and where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function"*

These standards recognise the need and importance of security awareness training and identify it as a necessary aspect of a successful Information Security Management System.

3.2.4 Benefits

The benefits of implementing an effective security awareness programme are well documented. The fundamental aspiration of Information Security Awareness is to make participants adopt safe computing practices [BM-08]. The aim of security awareness is to change behaviour and reinforce good security practice [NI-03]. An effective security awareness programme will help create and maintain security-positive behaviour [ISF-02]. It will reinforce the goals of the organisation and will ensure that the important messages will get to those who need them [TH-00, Ch 12 pg 200]. An effective programme will enable the participants to understand the relevance of information security for them and how it can help

them [TH-00, Ch 12 pg 197]. It will remind the participants not only of the risks they face but the countermeasures they can utilize to guard against them [TH-07, Ch 43 pg 522]. SANS state that,

> "*security awareness is an effective strategy to reduce the overall risk for an organisation. The more users are aware, the greater the chance their behaviour will be different, resulting in fewer negative incidents.*"

Research has shown that organisations that do not promote security awareness are at a higher risk of experiencing major security incidents than those that do promote awareness [ISF-02].

3.2.5 Difficulties

Implementing an effective security awareness programme can be a difficult task. There will always be obstacles and barriers to conquer. The following issues have been identified as those which impede the success of a security awareness programme;

- *Failure to follow up* [HT-00, ISF-02, E-08] – Many security awareness programmes are unsuccessful due to a lack of follow-up. Consistency is the key to a persuasive information security programme. Security awareness must be an ongoing activity and it is vital that the programme is kept alive and active. Regular communication with the audience is necessary to remind them of the key messages and to keep security issues at the front of their minds.

- *Failure to consider the audience* [HT-00, ISF-02, E-08] – Security awareness programmes that are designed without the audience in mind will not be successful. The messages and approaches of the programme must be relevant to the audience or the message will not be received.

- *Failure to explain* [E-08] – Another reason why security awareness programmes are unsuccessful is due to the fact that they fail to explain the reason and need for

implementing security measures. Users who understand why certain measures are required are more likely to comply.

- *Failure to employ an appropriate approach* [E-08, ISF-02] – In order for an information security awareness programme to be successful, the approach used must focus on changing behaviour. Through time users will have developed bad habits and providing them with knowledge only will not be sufficient in order for to change their ways. Programmes should recognise resistance to change and ensure that they use an approach that will aid behavioural change.

- *Failure to obtain management support* [E-08] – Security programmes will not succeed if they are not supported by senior management. This is one of the most crucial aspects for a security awareness programme.

Awareness of these obstacles and barriers ensures that they can be considered during the development of the programme and increase the chances of its success.

3.3 Developing an information security awareness programme

3.3.1 Approaches to a security awareness programme

The paper, **A Design Theory for Information Security Awareness [PP-06]**, identified 59 different approaches to security awareness that have been proposed over the years. These 59 approaches can be classified as either cognitive or behavioural with 15 of the proposed approaches utilizing both. The paper defines a cognitive approach to information security awareness as one that aims to change user behaviour through persuasive communication. It explains why compliance is required and believes that behaviour will not be changed unless the information is understood in a meaningful way. Behavioural approaches are founded in the theory that behaviour can be modified by changing environmental factors in response to undesirable behaviours. This is achieved through rewards for those who comply with information security requirements and punishment for those who fail to comply. The author of this paper has chosen to focus on cognitive approaches as she believes that this approach,

promotes long-term behavioural change which is required for a successful security awareness programme.

3.3.2 Cognitive approaches

"Building an Information Technology Security Awareness and Training Program" [NI-03] published by NIST, provides guidelines for building an effective information technology programme. The paper identifies three stages in the development of an IT security awareness programme; programme design, awareness and training material development and programme implementation. It also identifies the components of an awareness and training programme as mentioned in section 3.2.2. Advice and guidance is provided on a number of topics including performing a needs assessment, sourcing programme material, delivering techniques and methods to evaluate the programme. These guidelines propose three different approaches for designing, developing and implementing an awareness and training programme;

- *Centralized Program Management Model* assigns responsibility for the entire awareness and training programme to a central authority. This central authority carries out the needs assessment as well as developing the awareness plan and programme material. This model is generally used in organisations that are small and have similar objectives across the board.
- *Partially Decentralized Program Management Model* allocates the security awareness and strategy policy to a central authority with implementation consigned to line managers. Each line manager is responsible for development of programme material. This model is useful in larger organisation where organisational units have different needs.
- *Fully Decentralized Program Management Model* circulates the organisations policy and expectations on security awareness and training. A programme is designed, developed and implemented by each organizational unit. This model is helpful in large organisations where organisational units have diverse goals.

Figure 2 shows the model proposed by the **Information Security Forum [ISF-02]** for developing a security awareness programme. This is a four step model that results in the

design of numerous campaigns which can run side by side or in succession. Each campaign has a distinct design, development and delivery stage.

- Stage One – Objectives and goals are identified based on the problems to be solved. A risk assessment approach is suggested as a method to help define objectives for the programme as it provides a thorough, reliable approach for analysing the problems and identifying objectives to manage those problems.
- Stage Two – The scope and design of the programme is defined. An important aspect of this stage is preparing to change behaviour using Lewin's process of force field analysis.
- Stage Three – Security and awareness campaigns are developed and implemented.
- Stage Four – The effectiveness of the campaigns is measured.

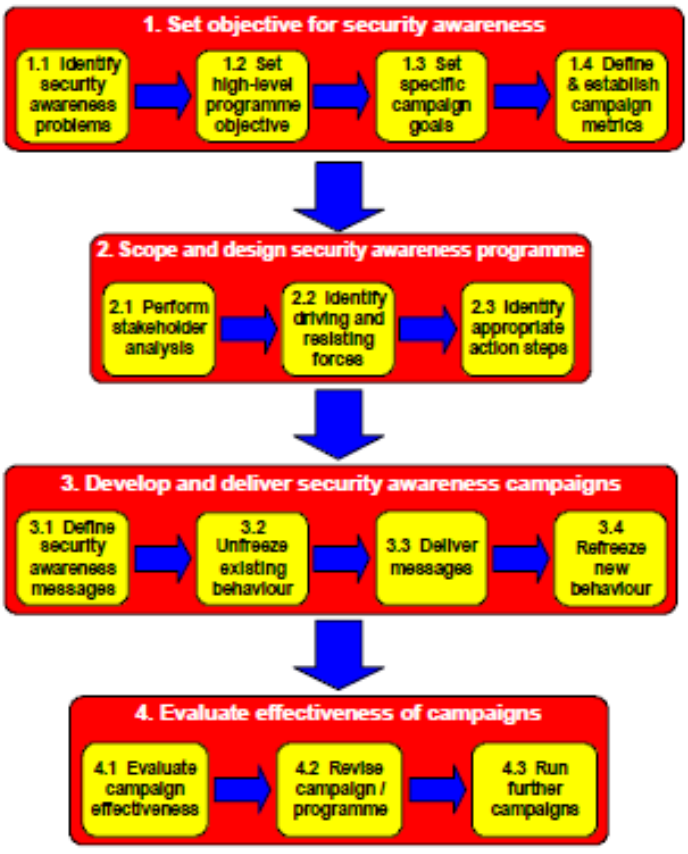

Figure 3.2 ISF for effective security awareness

[ISF-02]

The European Network and Information Security Agency (ENISA) is a centre of excellence for providing advice and guidelines on network and information security to European

member states and institutions. **The New Users' Guide: How to Raise Information Security Awareness [E-08]** describes a strategy for implementing an information security awareness programme. It also provides advice on the main factors to ensure success of an information security awareness programme. According to [E-08] an information security awareness programme consists of three main stages; plan, assess and design, execute and manage and evaluate and adjust [E-08]. Each of these stages is further divided into sub-processes as shown in Figure 3.3. In order to develop an effective information security programme these processes must be carried out.

- *Plan, assess and design* - An awareness programme must be designed to meet the organisational goals. The programme must be relevant for the organisation and the participants in the programme must deem its message important to them. This first process in the development of the awareness plan will identify the awareness needs, develop an effective awareness plan and attain the support of senior management.

- *Execute and manage* - This phase comprises of any activity that is necessary to put into operation the security awareness programme. This will include a needs assessment, strategy development, a plan for implementation of the programme and the development of required material.

- *Evaluate and adjust* - Evaluation and feedback are necessary components of a security awareness programme. The success of the awareness programme must be measured in order to identify its effectiveness and to identify any changes or adjustments that can be made to help improve further programmes.

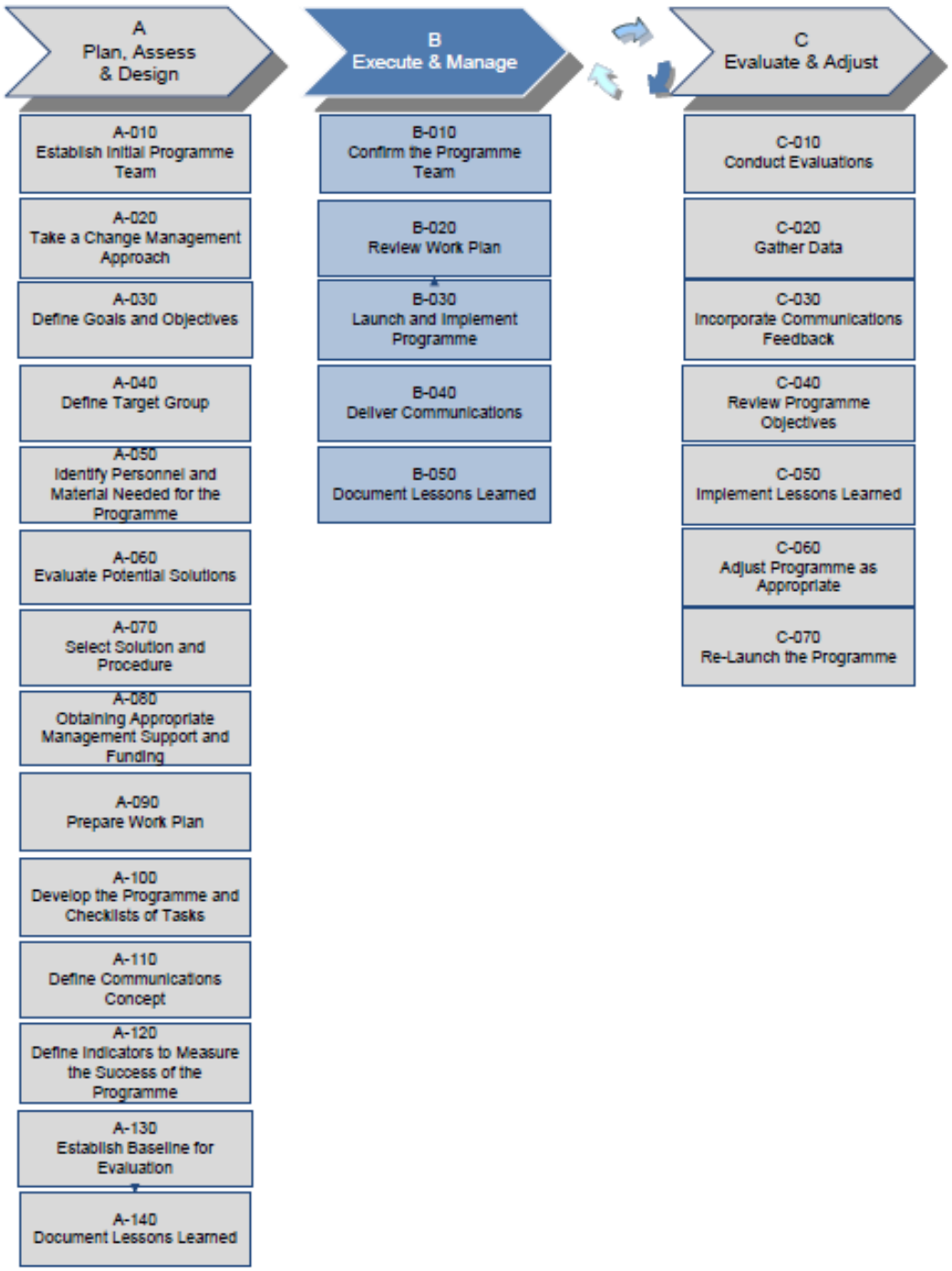

Figure 3.3 Phases of development of information security forum

[E-08]

3.4 Security awareness for children

3.4.1 Definitions and Concepts

It is important to define what security awareness means in terms of children. As this has not been documented before the opinions expressed here are those of the author.

By defining what security awareness means for children in terms of the ISF definition [see section 3.2.1], it is the degree to which every child understands the importance of information security and their responsibilities in achieving it, and based on this understanding, they are aware of and execute the appropriate actions. Using NIST's definition of an effective security awareness programme as stated in section 3.2.1, a security awareness programme for children will explain the proper rules of behaviour for using IT systems and information. Security awareness programmes are designed to change children's current behaviours and highlight good security habits.

Using the definition outlined in section 3.2.1, an effective security awareness programme for children can be described as a planned, meaningful learning process which will explain the proper rules of behaviour for using IT and information.

3.4.2 Components

The components outlined in section 3.2.2, will also apply when developing a security awareness programme for children.

3.4.3 Standards

There are no international standards for children that advocate explicitly the need for security awareness and training. However, the **Social Personal and Health Education Primary School Curriculum [D-99]** in Ireland contain some closely related objectives.

Under the strand unit of Media Education, the curriculum states that

> *"The child should be enabled to discuss and explore television, radio, videos, computer games, the Internet (worldwide web and email) and other media"*

The strand unit on Safety and Protection states that

> *"The child should be enabled*
>
> - *to adopt responsible behaviour at play and know the appropriate safety measures to take while playing*
> - *to identify people, places and situations that may threaten personal safety*
> - *to discuss a variety of risky situations and behaviour and assess and evaluate how these risks may be avoided or minimised and the implications of taking risks"*

The curriculum requires that children are given the opportunity to explore the Internet. It also requires that children are taught how to keep themselves safe at play and to develop the necessary skills to address risky situations. The way in which this can be achieved is through a security awareness programme and thus should be implemented in the school environment.

3.4.4 Benefits

A number of the benefits of implementing an effective security awareness programme as outlined in section 3.2.4 are also applicable to security programmes for children. They will make children adopt safe computing practices and will change behaviour and promote good security practice. The children will understand the relevance of information security and how it can help them. A good security programme will aim to make children aware not only of the risks they face, but also of the countermeasures they can utilize to protect themselves.

According to the **SANS Institute (SysAdmin, Audit, Network, Security)** "*security awareness training is an effective strategy to reduce the overall risk for an organisation. The more users are aware, the greater the chance their behaviour will be different, resulting in fewer negative incidents*." In applying this statement to children, one could conclude that the

more children are aware, the greater chance their behaviour will be different which in turn will result in a smaller number of security incidents involving children.

3.4.5 Difficulties

The difficulties outlined in section 3.2.5 will also apply when developing a security awareness programme for children.

3.5 Conclusion

In this chapter, a definition of security awareness and a security awareness programme was introduced. This was followed by the identification of the components, benefits and difficulties of security awareness programmes. The author then applied this theory to create a definition of security awareness and security awareness programmes for children. The components, benefits and difficulties of such a programme for children were discussed.

Guidelines for developing a security awareness programme for children have not yet been developed. Utilising the approaches described in section 3.3.2 and making appropriate changes to the processes and sub-processes the subsequent chapter presents guidelines for preparing and implementing an information security awareness programme that is suitable for use at primary school level.

Chapter 4
Security Awareness Plan

4.1 Introduction

Chapter Three outlines the components, benefits and difficulties associated with developing a security awareness programme for children. This chapter utilises the information and presents guidelines on how to develop such a programme for use in a primary school. It also outlines the details of the development of a security awareness programme for children aged between ten and twelve, the target audience of the author's own study. This is highlighted in italics throughout the chapter. Section 4.2 identifies the necessary processes for planning, assessing and designing the programme. Section 4.3 describes how to execute and manage the programme followed by evaluation and assessment guidelines in section 4.4.

4.2 Stage One: Plan, assess and design

The first process in the development of the awareness plan identifies the awareness needs of the school, develops an effective awareness plan and attains the support of principal, teachers and other members of the school community.

4.2.1 Establish a Programme Committee

There are many approaches to designing, developing and implementing an awareness programme as outlined in Section 3.3.2. It is the opinion of this author that a Centralised Program Management approach is most suitable to direct the development of an awareness programme in a school environment. This model assigns the responsibility for planning and organising the organisations security awareness programme to a committee. This committee is the motivating force behind the programme whose aim is to ensure that the plan is carried out. The members of the committee must be dedicated to the task as the effort they expend in planning, assessing and designing the awareness programme will determine its effectiveness. Suitable members for this committee are the school principal, teachers and expert parents.

The author will act as the programme committee for the purposes of planning and organising

the awareness plan proposed in this paper.

4.2.2 Assess the needs of the audience

Awareness programmes must be designed specifically for the audience they are targeting [E-08]. This is a critical factor for ensuring the success of the programme [Section 3.2.5]. In a primary school setting the various groups that can be targeted include the pupils, the parents, teachers, the classroom assistants and the other school employees. The needs of each group will be different and different methods of communication will be required in order to reach each group effectively. Each of the target groups must be analysed and the security risks that affect them identified. There will be some overlap between groups but vulnerability to the risk will differ as will the message and delivery mechanism [NI-98]. It is important to consider the experience and knowledge of each group independently. This information should include their Internet usage and online activities, their level of awareness of information security issues and their level of awareness of safety measures. This can be achieved by carrying out a survey and will ensure that the material in the campaign is pitched at the right level for the audience [NI-98].

An awareness programme in a primary school should be designed to target children, parents, teachers, classroom assistants and other members of the school community. The scope of the programme outlined here will only include children aged between ten and twelve years. In order to analyse this target group a self administered survey was distributed to four primary schools in the Republic of Ireland. The survey comprising of ten questions, was aimed at obtaining a general understanding of how children are using the Internet and their awareness of security issues and safety measures. A survey was also administered to parents of these children to gain a general understanding of parent's attitudes and habits regarding their child's Internet access and their awareness of some technological safety features. Teachers were also administered a survey to obtain evidence regarding teacher's use of the Internet with pupils and their knowledge of child e-safety initiatives already in circulation. (Full details of the methodology and results of the survey are contained in Appendix E and F)

The results of this survey identified that the most common activities that children use the Internet for are playing games (77.95% n=152), looking up information (40%,n=78), browsing for fun (36.92%, n=72), downloading (32.82%, n= 64), email (29.23%,n=57), social networks (22.56%, n=44), msn (13.85%, n=27) and making new friends (9.74%,

n=19). Using Table A, "Comparison of risks, activities and nature of Internet usage", the author identified the risks children may be exposed to while engaging in these activities. This is shown in Table B.

Almost half of the children surveyed are learning to use the Internet by themselves. Only 4.62% (n=9) declared that they learned to use the Internet from their teacher.

A*wareness of security issues and safety measures were mixed among the group. The belief that the Internet is not a safe place was held by over half of the sample population (54.36%, n=106). The most common reasons given for this related to one of the following categories; the ability of strangers to contact you, the risk of being cyberbullied, the ability of others to use your personal information for wrong reasons, inappropriate content and the fact that you may be influenced by what you see on the Internet. The remaining 45.64% (n=89) declared the Internet was a safe place because of the use of passwords, private profiles or anti-virus software. Eleven respondents declared that if you are careful the Internet is a safe place.*

These results indicate that children are divided in their opinion of the Internet. Although a number of the risks were identified by the group overall, not one respondent indicated a comprehensive understanding of all the risks. With regards to the children who declared the Internet was a safe place, only three technical measures were mentioned as a reason for this (passwords, anti-virus software and private profiles on social networking sites). This indicates a lack of awareness of other security measures that they can utilise to stay safe on the Internet. It also indicates a lack of awareness of their own ability to deal with the risks. The results of this survey indicate that overall children in this target group lack adequate knowledge of the associated risks and security measures.

4.2.3 Define programme objectives

Without accurate definition of the objectives it is impossible to plan an effective programme [E-08]. The guidelines of the ISF Model for creating a security awareness programme outlined in section 3.3.2 can be used to define the objectives.

1. Identify problems that can be addressed by a security awareness programme.
2. Establish high level programme objectives that address a problem previously identified.

3. Set specific campaign goals to define the purpose of each campaign.
4. Define and establish campaign metrics so that the success of the campaign can be measured.

This programme addresses the issue that children are frequent Internet users but lack the necessary skills and knowledge to enable them to manage the risks they face online.
The target group declared that they used the Internet on a regular basis, 75.25% with the most frequent response of use being everyday (28.22%, n = 57) [Appendix F]. The survey also revealed that children are unaware of all the security issues they face on the Internet and also of appropriate security measures. A security awareness programme can provide them with this knowledge and empower them to become responsible, safe Internet users.

The goal of the awareness programme is to enable children to become responsible, safe Internet users by raising their awareness of the risks they may face when online, and empowering them with the knowledge and skills to protect themselves. By analysing the activities children partake in according to the associated risks, three areas of concern are evident: safety, security and surfing skills [Table B]. Each of these areas will be targeted with individual campaigns.

Campaign One – Safety
The aim of the safety campaign is to equip children with the knowledge and skills they require to protect themselves online. The campaign will cover the topics of strangers, cyberbullying and netiquette.
Objectives: Following the programme the child will be enabled to • *Outline key Internet safety guidelines* • *Define the term cyberbullying and outline steps to deal with it* • *Explain the importance of keeping personal information private* • *Characterise safe online chat and messaging* • *Outline rules for appropriate behaviour online*

Campaign Two – Security
This campaign will teach children how to protect their computers and will focus on educating children about password usage, protection from viruses, spyware, phishing, spam and unknown emails.
Objectives: Following the programme the child will be enabled to • *Identify the need for passwords and outline steps to create a strong password* • *Choose appropriate screen names* • *Understand the terms virus, spyware, spam and phishing and be equipped with knowledge for managing these risks* • *Identify personal information that can be shared online and that which should be kept private.* • *Identify the appropriate steps to take in order to deal with attachments and e-mails from unknown senders, spam and free download offers.*

Campaign Three – Surfing Skills
The aim of the surfing skills campaign is to equip children with basic surfing concepts and provide them with the skills to deal with the various types of information they may find online.
Objectives: Following the programme the child will be enabled to • *Become familiar with suitable search engines and learn how to refine searches* • *Learn how to use the favourites folder to save their favourite sites* • *Analyse and critique information found on the Internet including commercial content* • *Identify steps to take if they encounter content that makes them feel uncomfortable*

4.2.4 Source material suitable for the programme

The material and resources required to run the programme must be identified. There is a wide selection of education resources on security awareness topics for children available on the Internet. Advice and information may also be gathered from other schools that have an awareness programme in place. There are also governmental organisations that develop suitable resources for primary schools. Once all the available materials are gathered it is important to identify the purpose of each resource and how each resource can benefit the programme. One possible method of achieving this is to classify the material in accordance with the message it contains.

Having identified the topics to be covered in each campaign it is necessary to create a compendium of resources available which can be utilised by class teachers. Table C contains a list of resources categorised according to the topic they cover.

4.2.5 Identify approach

Chapter 3 section 3.2.5 identified the difficulties that must be overcome in order to develop a successful awareness programme. Failure to employ an appropriate approach was one such difficulty mentioned. The aim of an awareness programme is to change behaviour and change attitude [NI-98]. In order for this to be realised the awareness programme must take a behavioural change management approach [E-08]. In a school setting this approach can be realised through particular teaching methods and mentoring activities. Beliefs and attitude have an effect on how we behave [TH-07, Ch 43, pg 522]. In order to change behaviour, teachers must consider pedagogy that addresses pupils existing beliefs and understanding. This model of pedagogy is known as conceptual change. It involves a process of identifying pupils preconceptions and encouraging them to revise their understanding based on new information received [NJ-82]. This method of pedagogy is very successful if the pupils find the new information reasonable, understandable and productive. It involves a four step process (1) Reveal student preconceptions, (2) Discuss and evaluate preconceptions, (3) Create conceptual conflict with those preconceptions, (4) Encourage and guide conceptual restructuring.

> *"When others are able to observe positive attitudes and actions towards aspects of a security awareness programme social proof can serve as a multiplier in encouraging positive behaviour."* [TH-07, Ch 43, pg 528]

Another method of achieving this in a school setting is through a mentoring scheme. Adept pupils can act as mentors for younger children during computer class. By observing positive security behaviour the younger pupils will be more inclined to imitate it. Teachers and other staff members can also demonstrate positive security behaviour for children.

An effective security awareness programme must be designed to accommodate for the fact that concentration levels decline during a presentation. The programme must therefore be creative, engaging and motivational with the main purpose being to focus the attention of the learner so that the learning will be included in conscious decision-making [NI-98].

Security awareness must be an ongoing activity and it is vital that the programme is kept alive and active [section 3.2.5]. E-safety ambassadors can help the awareness committee achieve this. An e-safety ambassador can be elected for each class grouping of the target audience. Those selected will be responsible for bringing the views of their classmates in relation to e-safety to the committee's attention. They will be responsible for completing mini-surveys among their peers and will also be a point of contact for classmates who may need advice or help. E-safety ambassadors will also be responsible for identifying ways to endorse e-safety among peers and for delivering e-safety messages at school assemblies.

The awareness programme must be creative and motivational in order to gain the attention of children. One means of engaging the children with the programme is to promote the programme with a mascot. The mascot will help get the message across and will build recognition with the children. For this programme Cyber Ed, a 12 year old inquisitive boy will be introduced and through him cyber security and safety issues will be presented. The children will be asked to help Cyber Ed solve problems he encounters and can email him with any queries or concerns they have.

4.2.6 Choose Methods of delivery

The next stage involved in planning the awareness program is to identify possible methods of delivery. A security awareness programme can be compared to a marketing campaign. Once customer needs are known, the next task is to select the products, modify it to suit the customer and then package it attractively. By delivering the right message to the audience,

using the most effective communication channel the interest of the audience will be captured and they will be persuaded to engage with the campaign [NI-98].

"*Communications is crucial for the success of any awareness programme*." [E-08]

There are many methods that can be elected to distribute the awareness message throughout the school. The method chosen will depend on the resources available and the complexity of the message [NI-03]. It will also depend on individual classes. Individuals learn in different ways and the approach most effective is one matching preferred learning style [NI-98].
Due to this the most effective ways to convey the campaign messages can vary from audience to audience and individual to individual. They can include posters, screensavers, assembly announcements, newsletters, teacher led training, peer presentations, security days, or web based sessions.

Expert speakers are another method of delivery that are suitable for use in a primary school. The International Information Systems Security Certification Consortium $(ISC)^2$ in conjunction with ChildNet International, a UK based children's charity have designed an education programme for children aged between 11-14 years. Certified members are willing to give presentations in their local primary schools. The programme focuses on the need to raise awareness of online safety and computer security and covers topics such as social networking, cyberbullying, viral emails, spam, identity theft and more. This delivery method will allow children to obtain advice from experts in the industry and provide teachers with up-to date information on the latest technology [SR-09]

4.2.7 Design the programme

A full list of topics to be covered in the programme must be identified and the objectives, message, delivery method and owner for each topic specified.

It is the opinion of the author that this phase of the programme should be carried out by each class teacher. As outlined in section 4.2.6 the awareness programme must be designed specifically for the needs of the audience. This includes considering preferred learning styles. Each class teacher will have knowledge of this and thus will be able to choose from the resources supplied an effective method of delivery.

4.3 Stage Two: Execute and manage

After gathering the appropriate resources and defining a plan it is now time to execute the programme and realise the goals and objectives set out previously. A clear explanation of the plan and activities must be given to all staff members who will be delivering the programme. They must understand their specific role and set of responsibilities for implementing the programme. The week leading up to the 11th September is Global Security Week and is the opportune time to launch a security awareness programme.

As mentioned in section 3.2.5, consistency is the key to a persuasive security programme and ongoing activity is vital in order to keep the programme alive. Once the programme is launched regular communication with the audience is necessary to remind them of the key messages and to keep security issues at the front of their minds.

In a school setting the programme will continue over the academic year with class teachers delivering lessons and messages but it is also important to highlight the main messages for the school audience at various stages. There are a number of initiatives already in place that schools can use to achieve this. Computer Security Day takes place in November to help raise the awareness of computer security issues and remind people to protect their computers and information. Safer Internet Day takes place in February to promote safe and responsible use of the Internet among children and young people. The school can also organise an e-safety week where a number of planned activities and events can take place.

4.4 Stage Three: Evaluate and adjust

In order to evaluate the accomplishments of the programme and to assess its performance feedback is required. Questionnaires, surveys and teacher observations are some ways to achieve this. The feedback gathered should be analysed and the findings used to adjust the programme as necessary.

Following the implementation of the programme in order to assess its accomplishments, it is suggested to re-administer the original survey and conduct interviews with the children to review their knowledge and skills in relation to cyber safety.

4.5 Conclusion

This chapter utilised the information presented in the previous chapters to produce a set of guidelines for developing a cyber security and safety awareness programme for use in a primary school. Section 4.2 outlines suggested steps to follow in order to develop the programme. Information on executing and managing the programme are set out in section 4.3 and section 4.4 suggests ways to assess the programme.

Unfortunately the author was unable to carry stage 2 of the programme as the primary schools were closed for the summer holidays. The schools that participated in the survey have expressed interest in implementing the final programme when the academic year begins again.

Chapter 5

Summary and Conclusions

5.1 Summary and conclusions

Three quarters of European children are online availing themselves of the numerous opportunities afforded by the Internet. It is an invaluable source of knowledge and encourages creativity and imagination. However alongside these opportunities are potential risks. This paper aimed to examine these risks and suggest a means of empowering our children with the necessary knowledge and skills to deal with them so that they can to reap the full benefits of the Internet and enjoy a safer online experience. This concluding chapter presents these findings.

Chapter Two analysed the existing research on the issues and risks children face on the Internet. It presented a classification of such risks with a description of each type. Those risks are of three types; content, contact and conduct. Content risks refer to risks in which the child is exposed to mass-distributed content. Contact risks refer to risks which may occur when the child is engaged in communication. Conduct risks relate to risks in which the child may be the initiator or actor of content or contact risks.

An examination of the nature of children's access habits revealed that children are using the Internet for four main reasons; communicating, learning, sharing and having fun. It also highlighted the fact that children's access patterns have changed. These changes include an increase in access from home, children accessing the Internet at an earlier age and an increase in the number of computers located in private places in the home.

The final section of this chapter used a risk management approach to identify a solution to enable children deal effectively with these risks.

The author believes that the numerous activities children partake in online, are providing them with excellent opportunities for learning and development. However these activities are also rendering children vulnerable to the contact, conduct and content risks outlined above. Evidence shows that the nature of children's Internet use is changing. The author believes that this give rise to an even greater likelihood that children will encounter risks online and it highlights even more the need to take a proactive approach in helping children deal with these risks. Dealing with risk is not a new phenomenon. Teaching children how to deal with risk is not a new phenomenon. However although parents are confident in their ability to teach their children to become competent risk managers in many areas of life, they feel powerless in helping their children develop the skills required to manage risks on the Internet. Without wanting to deprive children of benefiting from the many opportunities the Internet affords while protecting them from harm, necessary steps must be taken to enable them to become responsible Internet users.

In Chapter Two the author concludes that the most effective approach to help children deal with the risks they face online is to empower them with the necessary knowledge and skills they need to have a safer online experience. A security awareness programme designed specifically for children will achieve this goal. It will encourage children to adopt safe computing skills and will promote good security practice. It will aim to make children aware not only of the risks they face but of the countermeasures they can utilise to protect themselves. By empowering children with this knowledge, we can ensure that they will reap the full benefits of the Internet and enjoy a safer online experience.

Chapter Three focuses on security awareness and the development of a security awareness programme. It provides a definition of security awareness and discusses a number of related issues. These include components of a security awareness programme and the associated benefits and difficulties. It discusses the stages in the development of security awareness programmes and introduces some methodologies which are currently in use.

The author believes that this information can be utilised and adopted to define security awareness for children. The components and difficulties are applicable and the

methodologies currently in use can be modified to create guidelines for the development of a security awareness programme for children.

Chapter Four presents the authors set of guidelines for developing a security awareness programme for children. Included in these guidelines are details of the development of a security awareness programme for children aged between ten and twelve, the target audience of the author's own study.

Children face a number of risks on the Internet. They do not have the necessary skills to deal with these risks. It is crucial that children are empowered with the necessary knowledge and skills to enable them to utilise this fantastic resource in a safe, secure way. By educating children about the risks and issues they may face on the Internet, they will grow up with awareness and an understanding of these issues and this will help reduce the number of security incidents occurring due to the human factor in the future.

Using campaigns to heighten awareness of other issues have proven successful [DA-04]. We can therefore conclude that appropriate education and awareness programmes will be effective in increasing children's Information Security Awareness. Schools are a universal point of contact through which children can be reached. Thus it is vital that these programmes are put in place in all schools to enable our children to become safe, responsible Internet users.

In the past Information Security was a concern for computing professionals and government agencies only. With the ever increasing popularity of the Internet, it is now a concern for children and adults alike. By teaching them effective security and safety skills, we can ensure that they will reap the full benefits of this magnificent resource and enjoy a safer online experience.

> *"Providing information security is a huge challenge in itself; awareness raising among select target audiences is an important first step towards meeting that challenge."* [E-08]

Bibliography

[BM-08] Bishop, M., Irvine, C.; Teaching for Conceptual Change; IEEE Security & Privacy; November /December 2008 pg 67-69

[BT-08] Byron, T; Safer Children in a Digital World: The Report of the Byron Review; London; Department for Children, Schools and Families and the Department for Culture, Media and Sport; Retrieved from http://dcsf.gov.uk/byronreview/

[C-02] Cyberspace Research Unit; Young Peoples Use of Chat Rooms: Implications for policy strategies and programs of education; University of Central Lancashire; 2002

[DA-04] Delaney, A. et al; A Review of Mass Media Campaigns in Road Safety; Monash University Accident Research Centre; May 2004

[D-99] Department of Science and Education; Social Personal and Health Education Primary School Curriculum; Government of Ireland; 1999

[E-08] ENISA; The new users' guide: How to raise information security Awareness; 2008; available at http://www.enisa.europa.eu/doc/pdf/deliverables/newarusersguide.pdf

[EC-07] European Commission; Safer Internet for Children Qualitative Study in 29 European Countries Summary Report; May 2007; found on European Union website http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/qualitative_study_2007/summary_report_en.pdf

[FA-07] Fielder, A., Gardner, W., Nairn, A., Pitt, J.; fair game? : Assessing commercial activity on children's favourite websites and online environments; National Consumers Council; 2007

[FL-59] Festinger, L., Carlsmith J.; Cognitive Consequences of Forced Compliance; Journal of Abnormal and Social Psychology Volume 58 pg 203-210

[FO-09] Findahl, O; Preschoolers and the Internet: Will children start to use the Internet when they start walking?; World Internet Institute; EU Kids Online Conference; June 2009

[HU-07] Hasebrink, U, Livingstone, S, Haddon, L., and Ponte, C.; EU Kids Go Online: Comparing Children's Online Opportunities and Risks across Europe; 2007; available at www.eukidsonline.net

[HR-05] Herold, R.; Managing an Information Security and Privacy Awareness and Training Program; Auerbach; 2005

[IJ-96] Iivari, J.; Analyzing Information Systems Development: A Comparison and Analysis of Eight Development Approaches; Information Systems Volume 21(7) pg 551-575; 1996

[INF-09]

[ISF-02] Information Security Forum; Effective Security Awareness: Technical Report; Information Security Forum, United Kingdom; 2002

[ISF-07] Information Security Forum; The Standard of Good Practice for Information Security; Information Security Forum; United Kingdom; 2007

[ISO-05/1] International Standards Organisation; ISO/IEC 27001:2005 Information Security Management System – Requirements; October 2005

[ISO-05/2] International Standards Organisation; ISO/IEC 17799:2005 Code of Practice for Information Security Management; June 2005

[LS-09a] Livingstone, S and Haddon, L; Risky experiences for children online: Charting European research on children and the Internet; 2009, available at

http://www.lse.ac.uk/collections/EUKidsOnline/EU%20Kids%20I/Presentations/RiskyexperiencesCandS.pdf

[LS-09b] Livingstone, S, Staksrud, E, Haddon, L; What Do We Know About Children's Use of Online Technologies: A Report on Data Availability and Research Gaps in Europe; LSE, London: EU Kids Online, June 2009

[LS-09c] Livingstone Sonia; Children and the Internet; Polity Press; 2009

[LS-09d] Livingstone, S and Haddon, L; EU Kids Online: Final Report; LSE, London: EU Kids Online, June 2009

[N-03] NCTE; Children's study – investigating online behaviour; Safety Awareness Fact and Tools; May 2003.

[N-06] NCTE; Webwise 2006 Survey of Children's Use of the Internet; July 2006; from Webwise website www.webwise.ie

[N-09a] NCTE; 2008 Survey of Children's Use of the Internet in Ireland; January 2009; from Webwise website www.webwise.ie

[N-09b] NCTE; 2008 Watch Your Space Survey: Survey of Irish Teenagers Use of Social Networking Websites;

[NI-98] NIST; Information technology security training requirements: A role- and performance-based model, NIST — SP 800-16, USA, 1998, available at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

[NI-03] NIST; Building an information technology security awareness program, NIST — SP800-50, USA, 2003, available at http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

[NJ-82] Nussbaum, J., & Novick, N. (1982) Alternative frameworks, conceptual conflict, and accommodation: Toward a principled teaching strategy. Instructional Science, 11, 183-200

[O-03] OECD; Implementation plan for the OECD guidelines for the security of information systems and networks: Towards a culture of security, Working Party on Information Security and Privacy, OECD, 2003, available at http://www.oecd.org/dataoecd/23/11/31670189.pdf

[OD-89] Ostrow, D.; AIDS Prevention through Effective Education; Daedalus; Volume 18 (3) pg 229-254; 1989

[PP-06] Puhakainen, P.; A Design Theory for Information Security Awareness; Faculty of Science Department of Information Processing Science; 2006

[SC-09] Sádaba, Charo; The Interactive Generation in Ibero-America, Social and Educational Challenges; June 2009

[SE-08] Staksrud, E and Livingstone, S; Children and online risk: Powerless victims or resourceful participants?; available at http://www.lse.ac.uk/collections/EUKidsOnline/EU%20Kids%20I/Presentations/ChildrenAndOnlineRiskAoIRCopenhagen 2008.pdf

[SJ-89] Simpson, J.A., Weiner, E.; The Oxford English Dictionary Second Edition Volume 1; Clarendon Press, Oxford; 1989

[SM-08] Sharples, M et al; E-safety and Web 2.0 for children aged 11-16; Learning Sciences Research Institute, University of Notingham, UK

[SP-08] Smith, P., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., Tippett, N.; Cyberbullying: Its Nature and Impact in Secondary School Pupils; Journal of Child Psychology and Psychiatry; 49:4 2008 pp 376-385

[SR-09] Stringer, Rob; Get ‘em young; Info Security Magazine; volume 6(2); March 2009, pg 34-37

[TH-00] Tipton, H., Krause, M.; Information Security Management Handbook 4th Edition; Auerbach, 2000

[TH-05] Tipton, H., Krause, M.; Information Security Management Handbook 5th Edition, Volume Two; Auerbach, 2005

[TH-07] Tipton, H., Krause, M.; Information Security Management Handbook 6th Edition; Auerbach; 2007

[YL-96] Yngstrom, L.; A Systemic-Holisitic Approach to Academic Programmes in IT Security; Stockholm University; 1996

Appendix A

Table A: Comparison of risks, activities and nature of Internet usage

Risks		Activities leading to exposure	Nature of Internet access leading to increase in vulnerability
CONTENT	Age inappropriate content Pornography, racist content, harmful content	Playing games Researching topics of interest Browsing for fun Finding information for homework	Increase in frequency of access Self-learning
	Incorrect content	Finding information for homework Researching topics of interest Browsing for fun	Increase in frequency of access Self-learning Computer location
	Commercial content Advertising, marketing, spam,, sponsorship	Playing games, Browsing for fun Use of chat rooms and social networking sites	Increase in frequency of access Self-learning Age of child Computer location
CONTACT	Undesired contact Strangers, cyberbullying, online groomers,	Playing games Use of chat rooms and social networking sites Instant messaging	Increase in frequency of access Computer location
	Disclosure of personal information Strangers, identity theft, phishing, spam	Use of chat rooms and social networking sites Instant messaging	Increase in frequency of access Age of child Computer location
CONDUCT	Bullying or harassing another	Use of chat rooms and social networking sites Instant messaging	Increase in frequency of access Computer location
	Creating/uploading harmful material	Use of social networking sites	Increase in frequency of access Computer location
	Illegal downloads	Downloading music	Increase in frequency of access Age of child

Table B: Risk children may be exposed to according to online activity

Activities	Content Risks	Contact Risks	Conduct Risks
Playing games	Age inappropriate content Pornography, racist content, harmful content Commercial content Advertising, marketing, spam, sponsorship Disclosure of personal information Identity theft, phishing, spam Security Viruses, spyware	Undesirable contact Strangers, cyberbullying, online groomers,	Disclosure of personal information Identity theft, phishing, spam Bullying or harassing another Creating/uploading harmful material
Looking up information and browsing for fun	Age inappropriate content Pornography, racist content, harmful content Incorrect content Commercial content Advertising, marketing, spam, sponsorship Security Viruses, spyware		Disclosure of personal information Identity theft, phishing, spam
Downloading	Age inappropriate content Pornography, racist content, harmful content Security Viruses, spyware		Illegal downloads
E-mail	Commercial content Advertising, marketing, spam, sponsorship	Undesirable contact Strangers, cyberbullying, online groomers,	Disclosure of personal information Identity theft, phishing, spam Bullying or harassing another
Social networks and MSN	Age inappropriate content Pornography, racist content, harmful content	Undesirable contact Strangers, cyberbullying, online groomers, Disclosure of personal information Strangers, identity theft, phishing, spam	Disclosure of personal information Strangers, identity theft, phishing, spam Bullying or harassing another

Table C: Resources available online for security awareness programme

	Resource	*Safety*	*Security*	*Surfing Skills*
1	**Surfwise Internet Safety Module Age 6-10** www.webwise.ie "This learning resource introduces children to the characters of Niamh and Fionn as they learn to use the internet. This interactive cartoon demonstrates how to search the Internet safely and effectively, and outlines strategies for assessing the trustworthiness of online information. This module contains a teachers' guide, interactive digital resources, and classroom-activity worksheets."			●
2	**Chatwise Internet Safety Module Age 8 -12** www.webwise.ie "In this adventure of Niamh and Fionn, children learn how to use the internet to communicate safely and effectively with others. It raises awareness of the risks of sharing too much personal information online, good practice when communicating online, and strategies for dealing with spam. This module contains a teachers' guide, interactive digital resources, and classroom-activity worksheets."	●	●	
3	**Wild Web Woods Age 7-10** www.webwise.ie "The Wild Web Woods is an online game for teaching children basic Internet safety in a fun and friendly fairy tale environment. Mainly for children between 7 and 10 years of age. The object of the game is to reach a fabled E-city, but the paths travelled are fraught with mazes, dangers and tasks. Making one's way introduces basic Internet safety rules, as well as notions of human rights and respect for others."	●		
4	**How to keep safe while chatting online!** www.chatdanger.com "This site informs children of the potential dangers on interactive services online like chat, IM, online games, email and on mobiles. Children can read true stories and find out how to chat safely."	●		
5	**Digizen** www.digizen.org "Cybersmart provides activities; resources and practical advice to help young kids, kids, teens and parents safely enjoy the online world. Cybersmart has activities, animations, a quiz and facts about being cybersmart and cybersafe online It provides tips on how to stay safe in relation to cyberbullying, unwanted contact, inappropriate content, playing online, your digital footprint, netiquette and online friends."	●		

6	**Digizen** www.digizen.org "The section on young People and Social networking services provides information about using social network sites and social media sites creatively and safely. It provides tips for evaluating these online resources and examples of how to use them to support informal and formal learning. Responding to the range of risks faced by children and young people, Childnet has worked closely with the UK Government and a wide range of partners from the internet and mobile industries to produce practical advice and guidance on Cyberbullying. Let's Fight it Together is a short film based on a composite view of real events."	●		
7	**ThinkUknow** www.thinkuknow.co.uk This website provides tips on how to have fun, how to stay in control and how to report. It also provides information on Chatting, IM, email, mobiles, chat rooms, social networking, file sharing and gaming.	●	●	
8	**Captain Kara and Winston's SMART Adventure** www.childnet-t.org/kia/primary/smartadventure/ "Know IT All for Primary schools contains a specially designed five part 3D animation called 'The Adventures of Kara, Winston and the SMART Crew'. This film covers Childnet's five SMART rules which have been proven to be effective in helping younger children understand the importance of keeping safe online. Through their travels Kara and Winston use the internet, mobile phones, social networking pages and chat to negotiate and find their way through the adventure. Through their travels they are able to interact with a real life SMART crew of ten and eleven year old children who give instructions and help Kara and Winston stay safe."	●		
9	**CyberSmart!** www.cybersmartcurriculum.org/safetysecurity/ "CyberSmart! provides free non-sequential, lessons based on the most current research findings adopting best practices from the fields of cyber security and character education. Teacher lesson plans, student activity sheets, home connections, awareness activities and optional Web 2.0 strategies are included. Topics include handing passwords, spam, malware, phishing, and other forms of identity theft, communications, cyberbullying, protecting private identify information, making good search decisions and evaluating the resources they encounter online.	●	●	●

Appendix B

Questionnaire for children

Questionnaire for Pupils

Class: _____

Age: _____

Date: _____

Q1. How often do you use the Internet?

☐ Once a week	☐ Weekends only	☐ Rarely
☐ Everyday	☐ Never	☐ Other

Q2. Where do you access the Internet? (please tick all relevant boxes)

☐ At home	☐ In an Internet café	☐ In a friend's home
☐ At school	☐ In a relative's home	☐ Other

Q3. What do you use the Internet for? (please tick all relevant boxes)

☐ Playing games	☐ Looking up information	☐ Making new friends
☐ Browsing web pages	☐ Social Networks	☐ Downloading pictures/vid
☐ Messenger	☐ Email	☐ Other

Q4. What are your favourite websites? (please write the names of them here)

Q5. Who has shown you how to use the Internet?

☐ My parents/guardian	☐ My teacher	☐ Nobody, I learned myself.
☐ My brother/sister	☐ My friends	☐ Other

Q6. For which of the following pieces of information would you ask your parent's permission before sharing it on the Internet?

☐ Your name	☐ The name of your pet	☐ Your phone number
☐ Your school	☐ Your address	☐ Hair colour
☐ Your email address	☐ Your age	☐ A nickname

Q7. Do you have an email account?

☐ Yes	☐ No

If yes, do you open emails from people you do not know?

☐ Yes	☐ No

Q8. Do you have a profile on Bebo, Facebook or another social networking site?

☐ Yes	☐ No

If yes, is your profile private? (a private profile means that only your friends can view your profile)

☐ Yes	☐ No	☐ Don't know.

Q9. Do you think the Internet is a safe place?

☐ Yes	☐ No

Why do you think so?

_____
_____
_____
_____

Q10. Where is your favourite place to play?

☐ Inside	☐ Outside

Appendix C

Questionnaire for Parents

Questionnaire for Parents

Child's Class: _____

Child's Age: _____

Date: _____

Q1. How often does your child use the internet at home?

☐ Once a week	☐ Weekends only	☐ Rarely
☐ Everyday	☐ Never	☐ Other

Q2. Do you have separate user accounts on your home computer?

☐ Yes	☐ No

Q3. Do you have an anti-virus, anti-spyware or spam-filtering software on your computer?

☐ Yes	☐ No	☐ Don't know

Q4. Are the parental control features on your internet browser/operating system/email program enabled?

☐ Yes	☐ No	☐ Don't know

Q5. Do you teach your child to use a child-friendly search engine on your home computer?

☐ Yes	☐ No	☐ Was not aware that there are child friendly search engines

---

Q6. Do you monitor the websites your child visits?

☐ Yes	☐ No

Q7. Do you talk to your child about using the internet safely?

☐ Yes	☐ No

If yes, what issues do you discuss?

☐ Strangers on the internet	☐ Spam, phishing	☐ Using search engines
☐ Downloading material safely	☐ Sharing personal information	☐ Using passwords
☐ Other (please specify)	☐ Other (please specify)	☐ Other (please specify)

Q8. Have you received or researched any information on child e-safety initiatives?

Received information	☐ Yes	☐ No
Researched information	☐ Yes	☐ No

Q9. Would you like more information on how to teach your child to surf the internet safely?

☐ Yes	☐ No

Q10. As a child where was your favourite place to play?

☐ Inside	☐ Outside

Appendix D

Questionnaire for Teachers

Questionnaire for Teachers

Date: _____

Q1. Do you use the internet in school with your class?

☐ Yes	☐ No

Q2. Do you encourage your pupils to use the internet at home for further study?

☐ Yes	☐ No

Q3. Is the internet access in your school filtered?

☐ Yes	☐ No	☐ Don't know

Q4. As a teacher have you received or researched any information on child e-safety initiatives?

Received information	☐ Yes	☐ No
Researched information	☐ Yes	☐ No

If yes ,please specify

Q5. Do you teach your class specifically about internet safety?

☐ Yes	☐ No

If yes, please specify the content of what you teach

Appendix E

Methodology for survey

Overview

The aim of this study was to gain a general understanding of how children are using the Internet, to establish parent's awareness of child Internet safety and to identify if this topic is being taught by teachers. Self administered surveys were distributed to 4 primary schools in Ireland. There were three different surveys each designed for a different target audience; primary school pupils aged between 10 and 12, parents of these pupils and teachers.

Instrument

Although there is a wide availability of sample surveys previously designed on this topic, (ref) a new survey was designed by the author of this study. This survey was designed with the personal objectives of the author in mind. Consideration given to the fact that pupils were self administering the surveys and the difficulties known to be involved in gathering information from this audience. The survey instruments were developed following a literature review to enhance their content validity.

1) Survey for pupils aged 10 – 12 (Appendix B)
This survey comprised of ten questions and was aimed at gathering evidence on pupil's Internet habits; frequency of access, location of access, surfing habits and their awareness of certain Internet safety features.

2) Survey for parents (Appendix C)
This survey which consisted of ten questions was designed to gain a general understanding of parent's attitudes and habits regarding their child's Internet access and some technological safety features.

3) Survey for teachers (Appendix D)
This survey was designed to obtain evidence regarding teacher's use of the Internet with pupils and their knowledge of child e-safety initiatives already in circulation.

Pilot study

A pilot study involving five pupils aged between 10 and 12, five parents and five teachers established the face validity of the surveys and identified the need for minor amendments. The re-drafted survey was piloted on a further five survey respondents in each category. No problems with comprehension or completion were noted.

Sampling frame

Contact was made with previous university and work colleagues to ascertain their interest and availability to participate in the survey. The study population was divided into three categories; primary school pupils aged between 10 and 12, parents of the sampled pupil population and primary school teachers.

Procedure

In April 2009, approval for the study was sought and gained from the corresponding Board of Managements in each school. Each school appointed a co-ordinator to oversee the distribution and collection of the surveys.

In June 2009, surveys, a cover letter for the co-ordinator, a cover letter for the parents and a cover letter for the teachers were distributed to each primary school co-ordinator. Reminder emails were sent to the co-ordinators after a two week and four week period.

Data analysis

Data analysis was completed using Microsoft Excel. Data was entered into Excel spreadsheets, checked for errors by comparison with raw data, and cleaned as required. Data was then analysed using simple statistic formulas. Responses to the open survey questions were recorded manually and subsequently complied into frequency tables.

Appendix F

Results

Survey Response

Of the total of 253 surveys distributed to pupils aged between 10 and 12, 202 completed surveys were returned (74.8% response rate). Of the total of 253 surveys distributed to parents of these same pupils 111 were completed and returned (43.8% response rate). Of the total 60 surveys distributed to teachers 53 completed surveys were returned (88.3% response rate).

Descriptive Results

a) **Results of pupil's surveys**

Of the completed pupil's surveys, 7 declared that they never used the Internet. The subsequent responses of these seven were not included in the results analysis.

The majority of the pupils declared that they used the Internet on a regular basis, 75.25% with the most frequent response of use being everyday (28.22%, n = 57). Of those pupils who used the Internet everyday more than half were 12 years old (57.89%, n=33).

The most common location of access to the Internet was in the home, (88.72%, n=173), while school was the next most common location (34.36%, n=67) followed by a friend's house (24.10%, n=47) and a relative's house (23.59%, n=46). Only 5.13% (n=10) reported accessing the Internet at an Internet café.

The most common activities that children declared they used the Internet for were playing games (77.95% n=152), looking up information (40%, n=78), browsing for fun (36.92%, n=72), downloading (32.82%, n= 64), email (29.23%, n=57), social networks (22.56%, n=44), msn (13.85%, n=27) and making new friends (9.74%, n=19).

Many children claim to have learned to use the Internet by themselves (43.59%, n= 85). Parent/guardian was the next most common source of learning (33.33%, n=65) followed by siblings (10.77%, n=21). Only 4.62% (n=9) declared that they learned to use the Internet from their teacher.

In relation to email accounts over half of the sample population reported having an account (53.85%, n=105) and the large majority (82.86%, n=87) admitted they would open an email from someone they do not know.

Half the sample population have social networking profiles have social networking profiles (53.33%, n=104) and of those with a social networking profile the large majority had private profiles (62.50%, n=65) with 12.50% (n=13) responding that they were unaware as to whether their profile was private or public.

The belief that the Internet is not a safe place is held by over half of the sample population (54.36%, n=106). The most common reasons given for this related to one of the following categories; the ability of strangers to contact you, the risk of being cyberbullied, the ability of others to use your personal information for wrong reasons, inappropriate content and the fact that you may be influenced by what you see on the Internet.

The remaining 45.64% (n=89) declared the Internet was a safe place because of the use of passwords, private profiles and anti-virus software. A number of respondents declared that they believed that if you are careful the Internet is a safe place.

The majority of children, 83.08% (n=162) chose outside as their favourite place to play.

b) Results of parent's surveys

One quarter of the parents surveyed believed that their children used the Internet everyday (25.23%, n=28). A very small minority reported that their child never used the Internet, (4.50%, n=5).

Almost half of the sample population have configured the separate user accounts on their home computer, (48.65%, n=54) and the majority of respondents, (90.99%, n=101) declare that they use an anti-virus, anti-spyware or spam-filtering software on their computer.

Parental features on their Internet browser, operating system and email program were enabled by over half of the sample population, (52.25%, n=58). Almost one fifth (18.02%, n=20) admitted that they did not know if the parental features were enabled with 29.73% (n=33) responding that the features were not enabled.

Almost one fifth of the parents surveyed (18.92%, n=21) admitted that they did not teach their child to use a child-friendly search engine. An overwhelming 45.05% (n=50) of parents responded that they were unaware that such search engines existed. Only 36.04% (n=40) responded that they actively taught their child to use a child-friendly search engine.

Websites that children visited are monitored by the majority of parents who took part in the survey, (86.49%, n=96). The study revealed that 93.69% (n=104) of parents surveyed discuss Internet safety with their child. The most common issues discussed were sharing personal information, (72.97% n=81), strangers on the Internet, (72.07%, n=80), downloading material safely, (58.56%, n=65) and using passwords, (39.64%, n=44).

A large majority of the sample population revealed that they never received information (81.08% n=90) or researched information (87.39% n= 97) on child e-safety initiatives. 80.18% of the parents responded that they would like more information on how to teach their child to surf the Internet safely.

The favourite place to play as a child for the majority of parents surveyed was outside (92.79%, (n=103).

c) Results of teacher's surveys

Of the teachers sampled, 79.25% (n=42) responded that they use the Internet with their class and that they encourage the children to use the Internet at home for further study.

The majority of respondents (84.91%, n=45) were aware that the Internet access in their school was filtered with a very small minority (3.77%, n=2) replying that they did not know whether the Internet access was filtered or not.

One third of the teachers responded that they had received information on child e-safety initiatives (33.96% n= 18) with two thirds replying that they did not receive any. Almost all teachers who participated in the survey (92.45% n=49) replied that they did not research information on such initiatives.

Only 15.09% (n=8) of respondents reported that they taught their class specifically about Internet safety. The main content taught by those 15.09% is in relation to advising children about pop-ups, basic chatting rules and use of personal information.