Security Awareness for Children

Young children can benefit hugely from early exposure to technology, but they can also be harmed by it. **Clara Brady** and **Chris Mitchell** explain some of the problems, and outline how security awareness programmes can work effectively.

Royal Holloway University of London

SearchSecurity.co.UK

abstract

This article 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.

1. INTRODUCTION

THE INTERNET plays an increasingly larger role in the everyday lives of our children. As a learning and communication tool, it offers them a wide range of opportunities [SGHL08]. 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 [LH09].

Unfortunately, Internet use also carries risks, ranging from exposure to inappropriate content, undesirable contact from strangers, and even cyberbullying, which children may not have the necessary skills or knowledge to manage [B08]. 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 [N09] 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 [B08]. 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.

Section 2 provides a brief overview of the categories of online risks for children. In Section 3 the findings of a survey conducted to gather evidence on the nature of children's Internet access are discussed. This focuses on children's surfing habits and their awareness of certain safety features. Section 4 outlines the objectives of an awareness programme for children and the paper concludes with Section 5.

2. ONLINE RISKS FOR CHILDREN

The EU Kids Online network classifies online risk for children into three categories – content, contact, and conduct [HLH08]. Children are also vulnerable to the security risks that all Internet users encounter.

- **Content** risks refer to those risks that may occur when the child is exposed to mass-distributed content. Examples include age inappropriate content, incorrect content and commercial content.
- **Contact** risk refers to risks which may occur when a child is engaged in online communication, such as undesirable contact and cyberbullying.
- **Conduct** risks relate to risks in which the child is the initiator of content or contact risks. These types of risk include bullying and harassing other children, creating/uploading incorrect or harmful material, and illegal downloads.
- **Security** risks include viruses, spyware, spam, identity theft, disclosure of personal information, and phishing.

Evidence shows that children are accessing the Internet more frequently [LH09], making it more likely they will encounter the above risks. Therefore, we must take a proactive approach and provide our children with the skills they require to deal with these risks. An awareness programme for children is needed.

3. SURVEY FINDINGS

A self-administered survey was distributed to four primary schools in the Republic of Ireland to determine how children aged between ten and twelve years are using the Internet. The

survey, which was completed by 202 children, consisted of ten questions and was designed to gather evidence on the nature of children's Internet access, the location of access, children's surfing habits and their awareness of safety measures.

Overall the survey revealed that children are established Internet users availing themselves of the many opportunities the Internet provides.

The survey revealed that 77.95% of children use the Internet for playing games, 36.92% browse the Internet, 32.82% use the Internet to download music, 29.23% use it for email, 22.56% for social networks, 13.85% for instant messaging and 9.74% for making new friends.

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

Half the sample population have social networking profiles (53.33%) and of those with a social networking profile the large majority had private profiles (62.50%) with 12.50% 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%). 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 inappropriate reasons, inappropriate content and the fact that you may be influenced by what you see on the Internet. The remaining 45.64% declared the Internet was a safe place because of one of the following reasons: the use of passwords, private profiles or anti-virus software. A number of respondents declared that if you are careful the Internet is a safe place.

Overall the survey revealed that children are established Internet users availing themselves of the many opportunities the Internet provides. It also revealed that a number of children in the group are aware of some of the security issues and safety measures they face. Although a number of risks were identified by the group overall, not one respondent indicated an awareness of the range of risks. Similarly, the findings revealed

TABLE 1

RISKS CHILDREN MAY BE EXPOSED TO DUE 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*

an inadequate knowledge of the range of skills and means required to deal with the risks they face online. These findings highlight the need for an Information Security Awareness programme for children so that all children are equipped with the necessary skills and knowledge to have a safer online experience.

4. PROGRAMME OBJECTIVES

An awareness programme must be designed specifically for the audience it is targeting [EO8]. This is a critical factor for ensuring success of the programme [EO8]. The target audience must be analysed and the issues they face online identified. In this paper, the author achieved this, by conducting a survey as described in Section 3.

Table 1 (see page 5), indicates the risks children aged between ten and twelve face based on their online activities. It was compiled using the risks identified in Section 2 and the findings of the survey described in Section 3. It is evident from this, that skills to deal with age-inappropriate content, commercial content and undesirable contact must be included in the awareness programme. Other concerns that arise are disclosure of personal information and cyberbullying.

As the majority of children are learning how to use the Internet by themselves, it is unlikely that they will adopt safe computing habits unless they are taught by a proficient user. The awareness programme can introduce safe behaviour.

The finding that the majority of children would open an email from someone they do not know indicates the need to educate the children about safe use of emails, including how to deal with emails from unknown senders and those with attachments.

The finding that the majority of children would open an email from someone they do not know indicates the need to educate the children about safe use of emails, including how to deal with emails from unknown senders and those with attachments. It was clear from the survey that not all children understand the importance of keeping their profile private

on social networking sites. This is a concern and must also be addressed in the awareness programme.

The above findings highlight some of the knowledge and skills that children aged between ten and twelve need to have a safer online experience. I believe that three different awareness campaigns are necessary to address these. The campaigns will raise children's awareness of the risks they face online and educate them about the safety and security issues they may encounter.

Each campaign should aim to achieve the following objectives:

Internet Safety

The aim of this 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 appropriate online behaviours. Internet safety guidelines covering safe chat and safe messaging should be introduced. The importance of keeping personal information private and steps to deal with cyberbullying must also be covered.

Following this campaign 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.

Internet Security

The security campaign aims to educate children on how to protect their computers and information. It will focus on password usage, protection from viruses, spyware, phishing, and unknown emails.

Following the campaign the child will be enabled to:

- Identify the need for passwords and outline steps to create a strong password.
- 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 email from unknown sources, spam and free download offers.

HOME
THE INTERNET AND CHILDREN
SURVEY FINDINGS
TABLE OF ONLINE RISKS
DESIGNING A PROGRAMME
CONCLUSIONS
REFERENCES

Surfing Skills

The final campaign aims to provide children with basic surfing concepts and provide them with the skills needed to deal with the various types of information they will find online.

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.

There are already some excellent awareness resources in existence which can be used to implement different aspects of the above campaigns. Webwise, the Irish Internet Safety Awareness Node of Insafe has developed educational resources about the potential risks on the Internet and aims to raise awareness among parents, teachers, and children. It focuses on safe surfing, safe chatting and safe sharing. Know IT All for primary schools, developed by the children's charity ChildNet, uses a 3D animation to introduce five SMART rules to help children understand the importance of staying safe online. Information on other existing resources can be found in the full MSc report. These resources are invaluable and will greatly enhance the success of an awareness campaign.

5. CONCLUSIONS

Using campaigns to heighten awareness of other issues have proven successful [DLWC04]. 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. ■

ABOUT THE AUTHORS

Clara Brady is a qualified primary school teacher from Ireland. Alongside her teaching degree she studied Mathematics as an academic subject and this is where she first encountered Cryptography. After a number of years teaching, she decided to further her interest in this area and returned to university to study the MSc in Information Security.

She has organsied a Security Awareness Day for her school, and hopes to build on this next year and to continue to highlight and promote the need to educate children about using the Internet in other schools throughout Ireland.

Chris Mitchell is a Professor of Computer Science at RHUL. His main research interests are in information security and combinatorial mathematics.

REFERENCES

[B08] 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/

[DLWC04] Delaney, A, Lough, B, Whelan, M and Cameron, M; A Review of Mass Media Campaigns in Road Safety; Monash University Accident Research Centre; May 2004

[E08] ENISA; The new users' guide: How to raise information security awareness; 2008; available at http://www.enisa.europa.eu/

[HLH08] Hasebrink, U, Livingstone, S, Haddon, L.; Comparing Children's Online Opportunities and Risks across Europe: Cross-national comparisons for EU Kids Online London 2008; available at www.eukidsonline.net

[LH09] Livingstone, S and Haddon, L; EU Kids Online: Final Report; LSE, London: EU Kids Online, June 2009

[N09] NCTE; 2008 Survey of Children's Use of the Internet in Ireland; January 2009; from Webwise website www.webwise.ie

[SGHL08] Sharples, M, Graber, R, Harrison, C, and Logant, K; E-safety and Web 2.0 for children aged 11-16; Learning Sciences Research Institute, University of Nottingham, UK