E-Safety in the Mobile Context

A. Legunsen and S. Atkinson

Centre for Security, Communications and Network Research
Plymouth University, United Kingdom
e-mail: info@cscan.org

Abstract

The research aims to develop practical strategies which can be used to curb dangers and risks associated with children going online through mobile devices. The research identified that stakeholders have a role in ensuring e-safety so a multi-stakeholder practical approach was employed and it entailed using a data survey conducted by Plymouth Safeguarding Children‟s Board. A risk model was also developed for the purpose of implementing practical strategies to minimize online risk. The data from the survey was analysed and the risk model was implemented on the outcome of the survey. The risk model discovered inherent problems in particular situations and the different stages of the risk model are applied to the problem until a positive feedback resolved the problem.

Keywords

Mobile, E-Safety, Risk Model

1 Introduction

The primary essence of technology, of which the internet and mobiles are by-products, is to add positive effects to life. The internet, which can now be accessed from a range of mobile devices including mobile phones, handheld game consoles like the Nintendo DS, Sony‟s PSP, and Apple‟s iPod touch, has become an integral part of modern family living. The use of technologies on mobile platforms has increased tremendously and children are increasingly having their own internet enabled mobile devices. Although these devices present children with opportunities in learning, socialising and entertainment, they also expose them to certain risks. Of note are the likes of cyber bullying, identity theft, access to pornographic images and videos, sexting, exposure to strangers, spam, viruses, abuse of intellectual property and even excessive use (Livingstone et al., 2011).. Internet safety measures are often implemented in schools and homes to guide young people online but managing the implementation of such safety measures within the mobile content has proved to be a daunting task.

This research aims to develop practical strategies which can be used to curb the dangers and risks associated with children going online through mobile devices. The research will investigate the present modalities in place for ensuring e-safety in the mobile context, the shortcomings of such modalities, and finally, a risk model will be designed to aid the implementation of practical strategies that end users can follow in order to minimize the risks.

2 Background

Surveys on e-safety started as early as 1999 when Finkelhor et al. (2008) conducted the first youth internet safety survey (YISS-1) with 1,501 youths within the age range of 10 to 17 years. Of recent, there have been diverse researches on cyber-bullying, online sexual harassment, and exposure to pornographic materials amongst adolescents. Researches have also considered the ways in which the society is making efforts to reduce these online risks, especially through parents and schools.

Major concerns have also risen based on the increase in statistics of mobile device ownership and usage amongst children. 50% of 10 year olds in most EU countries already have a mobile phone while 75% of 6 – 17 year olds are already active online (EC, 2008a; Livingstone et al., 2009). Recent statistic for the EU Kids Online project show that 60% of kids between 9 – 16 years go online daily, spending an average of 88 minutes online per day, and 33% of these kids go online via a mobile phone or other handheld devices (Livingstone et al., 2011). These show the extent of growth in the use of mobile amongst children in recent years and forecasts by Cisco (Cisco, 2011) showing further growth is inevitable necessitates the need for adequate e-safety measures in mobiles.

Mobiles and online technologies present young ones with opportunities for learning, socialising, and entertainment but exposure to risks such as cyberbullying, meeting online contacts offline, giving out personal information, sexual and online harassments, hacking, and mobile malware attacks also accompany these opportunities (Donoso et al., 2009). With these risks comes the need to ensure e-safety.

2.1 Who is to ensure e-safety?

To ensure e-safety, the question of who is responsible for e-safety needs to be clarified. Livingstone et al. (2009) and Byron (2010) agreed that the responsibility of ensuring e-safety lies with the multiple stakeholders involved. This includes the young ones that use the mobile device, the companies that manufacture the devices, mobile network operators and ISPs, security community and web programmers, governments, teachers and also parents.

2.2 Byron Review

The Byron Review (Ofcom, 2007) identifies a similar set of stakeholders and places them in a value chain. Two types of control were identified and implemented along the value chain. These are – controlling the availability and controlling the access to potentially harmful contents. Byron provided an update to these control measures in 2008 (Byron, 2008) by adding children"s resilience to harmful and inappropriate content online.

3 Adopted Practical Approach

An area of the Byron review was considered in choosing a practical approach to ensuring e-safety in mobiles. Byron mentioned a list of education-based initiatives to help promote e-safety awareness. One of these initiatives is the need to have Local Safeguarding Children Boards (LSCB). Their objective is to "coordinate and to ensure the effectiveness of their member agencies in safeguarding and promoting the welfare of children" (Ofcom, 2007). LSCB are also expected to deploy a multi-agency approach to e-safety. This makes this adopted practical approach robust as the board can provide details about other stakeholders.

The adopted practical approach uses an Early Years Survey carried out by the e-safety group of the Plymouth Safeguarding Children Board (PSCB) in collaboration with Plymouth University. The survey was conducted in April 2010 by Dr Shirley Atkinson from the School of Computing and Mathematics, Plymouth University. The aim of the survey was to gain an accurate picture of the online use of children under the age of 5.

The survey was implemented using questionnaires. This was made available in hard copy during an e-safety training session. The data gathered was analysed using both quantitative and qualitative methods.

4 Risk Model for E-Safety in Mobiles

The primary innovation of this research is the design and development of a risk model for e-safety in mobiles. The research carried out reveals there is presently no risk model designed specifically for the purpose of e-safety in mobile devices. The solutions available are models geared towards e-safety in general such as BECTA"s PIES model (BECTA, 2008) and the 360 degree safe self review tool by SWGfL (SWGfL, 2011).

The main aim of these models is to help develop and review policies and practices regarding online safety for children and young ones. These policies are instructions to guide the users and also to educate the guardians on how to ensure that young ones are safe online. However, the success of policies lies in its adherence. Therefore having policies in place does not necessarily guarantee acceptance and adherence by the users. Also, risks inherent in mobile situations are unique and not easily guarded by general policies but specific practical strategies. The models, therefore, need to be further backed up by practical strategies, and this research aims at achieving this with the implementation of the developed risk model.

The essence of the risk model is to capture a measure of the reality of risks inherent in the mobile context. Figure 1 show the risk model designed towards putting a check in the e-safety process in mobiles. This model takes changes in technologies into consideration as this is a common occurrence in the case of mobiles.

In a bid to develop and design this risk model, the models presented by BECTA and SWGfL were considered as guidelines but streamlined to a mobile-inclined perspective.

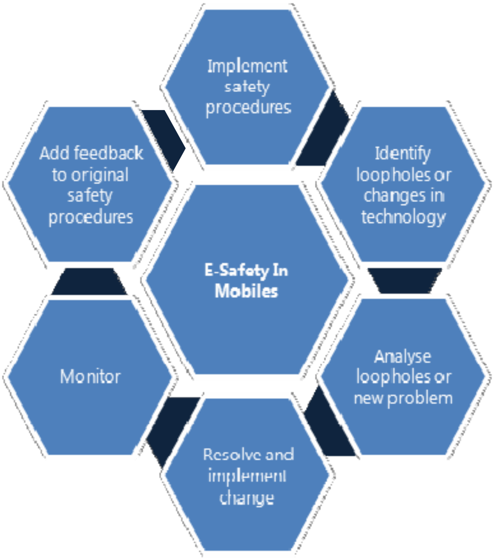
Implement safety procedures
Identify loopholes or changes in technology
Analyse loopholes or new problem
Resolve and implement change
Monitor
Add feedback to original safety procedures
E-Safety In Mobiles

Figure 1: Risk Model for E-Safety in mobiles

The policies and practices advised by these models form a part of the first step in the model. The set of safety procedures that apply to mobiles are highlighted and implemented. This model examines the present effects of the implementation of these safety procedures and proceeds into considering the loopholes that might exist in these procedures. Afterwards, the identified loophole, which could be as a result of change in use patterns or even a new technology, is analysed in depth.

Based on the outcome of the analysis, suggestions are worked out with the aim to achieve a safe procedure once again. This could necessitate an adjustment in the e-safety policy, the need to provide further training, or other measures. The change is then implemented and a period of monitoring is stipulated. During this period, the effect of the change implemented against the identified loophole is observed closely.

The feedback obtained can be treated in two ways. If it is positive, it can be fed directly into the original safety procedure and a more secure e-safety measure is attained. On the contrary, if the feedback obtained is negative, it can be fed back into the „analyse" or „resolve and implement" sections. This is further reviewed, the result is implemented and monitored, and when the feedback becomes positive, it is added to the original safety precautions.

5 Survey Results and Implementation of Risk Model

The result obtained from the Early Years survey is analysed using quantitative and qualitative research methods. An Early Years toolkit developed by the PSCB and the final policy recommendation for EU Kids Online project by Dr Sonia Livingstone and the EU Kids Online network are used as a check on the outcome of the survey"s data analysis. The outcome of the data analysis is discussed as a means for the implementation of the risk model.

5.1 The Early Years Survey

There were a total of 151 respondents to the survey in 106 days between 7 July 2010 and 20 October 2010. The survey required the participants to fill a questionnaire with about 15 questions addressing the use of technologies such as mobile devices and internet in their Early Years settings. The questionnaire also inquired about their practice of online safety, mobile phone usage staff"s ability to use online technologies safely, how secured their ISPs are, and the awareness and adoption of an Acceptable Use Policy.

5.2 Discussion and Implementation of the Risk Model

5.2.1 ISPs

ISPs can play a major role in achieving e-safety in mobiles by blocking illegal contents, filtering services, and providing useful information about online safety to parents and children (Ofcom, 2007). End users need to verify that the services provided by their ISPs are secured, and in this regard, the different means of connectivity should be considered. If the ISPs carry out the responsibility of blocking and filtering adequately, then a secured connection can be provided to end users which in turn promotes e-safety.

The first step of the risk model is to implement safety procedures and considering ISPs, data from the survey shows that most settings have a secured internet connection. 91% confirmed that there ISP is a recognised name and 82% of these mention that their internet connection is also secured. This information suggests that most of the ISPs have implemented suitable safety features in their services. With the first level of the risk model satisfied, this area of e-safety can be judged satisfactory. However, the services by the ISPs need to be monitored still as updates on services or upgrade of equipment could open up new vulnerabilities.

5.2.2 Acceptable Use Policy

The availability and awareness of an Acceptable Use Policy (AUP) is deemed as the minimum level of adoption by the settings towards online safety but the survey revealed only half of the settings have an AUP. The absence of an AUP means there is likely to be no agreed way of handling situations within the setting which could in turn affect other online safety requirements in the setting. This is further proven by the data survey as 51% mention that they have no designated person for online safety. In the same light, the awareness of the AUP by all staff and parent is not satisfactory with just 23% strongly agreeing to the question.

BECTA"s PIES model and the 360 degree safe models are built on developing policies and practices but having a standard policy does not guarantee its successful implementation. Acceptance and adherence by users is prime. This being a shortcoming of these models is proven by the survey, with 24% stating out rightly that they have no AUP and 20% do not know if one exists in their setting or not.

However, haven identified an unsatisfactory state in the implementation of the Acceptable Use Policy as a safety procedure, and also recognized the loophole as being an absence of the policy or lack of awareness by staff and parents, this loophole is analysed further. The reason for the absence of the AUP or lack of awareness needs to be investigated and corresponding measures taken to resolve the problem. With respect to policy development and implementation, Albrechtsen and Hovden (2010) recommend a workshop approach which involves the parties concerned. Rather than presenting a „finished" document and presenting it to the parties to accept and adhere to as the AUP, Albrechtsen and Hovden recommend that the parties adopt dialogue, participation and collective reflection during the policy development. Such approach can be implemented as a measure to resolve the problem. A monitoring period is stipulated to monitor the use of the new AUP and appropriate feedback is carried out on the process. The risk model can also be applied in the same manner to policies that fails to address a situation appropriately.

5.2.3 Mobile Phone Usage

Another area of concern raised by the survey is the management of mobile phone in the Early Years settings. Most of the settings do not permit the use of mobile phones in their settings with 60% stating this clearly. This step is taken by some settings in a bid to ensure safety, but as discussed in the technology use section, taking extreme measures such as completely banning mobile phones to reduce risk can in turn prevent opportunities. Banning technology could have a negative impact on learning. Children are supposed to be educated and trained on the use of technology and not denied its use.

Also, the use of mobile phones has become an integral part of daily living and placing a ban on its use in settings might result into members of the setting trying to get around the rules. This can yet have further impacts on learning in the setting. The implementation of the risk model in this case helps to identify the loophole and implement safety procedures unique with each setting.

5.3 Scenarios of the Risk Model Implementation in Mobiles

The implementation of the e-safety risk model in mobile-specific scenarios shows how the risk model can help to further check inherent risks after the implementation of standard policies. Present day mobile operating systems are now being accompanied with online application stores. Examples include Apple"s App Store, Google"s Android Market, BlackBerry"s App World and Windows 7 Marketplace. Young ones can download resources such as games, music and software from these stores but these exposes them to the risk of downloading malicious applications or their financial information might be stolen and used for fraudulent purposes. Kaspersky (2011) reported the detection of over 50 malicious Android OS applications which were written and distributed through the Android market by cybercriminals. The implementation of the risk model in such situation identified loopholes with the content producers.

Another scenario is the use of social networking sites (SNS) on mobiles by young ones. SNS often carry out upgrades on their sites, bringing in new features which leave the user‟s settings to the default state set by the SNS. These changes often happen without prior notification and users, especially young ones, might likely continue to use the SNS‟s new features without considering if new risks are associated with such features. Usage on mobile devices sometimes makes these changes unnoticeable. Dangers associated with such changes needs to be examined to prevent young users from being exposed to the associated risks.

6 Conclusion

This research was carried out with the aim of developing practical strategies which can be used to curb the dangers and risks associated with children going online through mobile devices.

Analysis of the data gathered was criticized with the Early Years toolkit and the final recommendation policy, and the results were discussed and used to evaluate the designed risk model. Results showed that even though the Early Years settings that participated in the survey were aware of the policies and practices available in the Early Years toolkit to help ensure online safety in their settings, they still did not adhere to some of the prescribed practices.

Rather than a policy which is developed after carefully considerations of, supposedly, all possible scenarios, the developed risk model addresses the situation in accordance with its present context. Policies provide instruction and guidelines to help in the decision-making process of problem solving. The e-safety risk model, however, helps to check inherent risks in mobile situation after the implementation of the policies. As shown from the scenario, policies can guide young ones in the general usage of social networking sites for example, but addition of new features which is not covered by the present policy in place can introduce new vulnerabilities and risk. The e-safety risk model can be used to analyse such situations and implement new safety procedures within a short period rather than the daunting task of reviewing the policy.

6.1 Future Work

This research gives room for further evaluation and implementation of the risk model. Effort can be made to implement the risk model in a setting or institution working towards improving the state of e-safety in mobiles. Another area of further research is the opportunity to carry out surveys with other stakeholders, using the data collated to examine the implementation of the risk model.

7 References

Albrechtsen, E. and Hovden, J. (2010) „Improving information security awareness and behaviour through dialogue, participation and collective reflection - An intervention study‟, Computers & Security, 29(4), pp. 432-445. [online] doi:10.1016/j.cose.2009.12.005 [Accessed 10 December 2011].

BECTA (2008) Safeguarding children in a digital world: developing an LSCB e-safety strategy. Available at: https://www.education.gov.uk/publications/standard/_arc_SOP/Page11/BEC1-15535 [Accessed 28 December 2011].

Byron, T. (2010) Do we have safer children in a digital world? A review of progress since the2008 Byron Review. Available at: http://www.education.gov.uk/ukccis/about/a0076277/the- byron-reviews [Accessed 26 December 2011].

Byron, T. (2008) *Executive summary of the 2008 Byron review.* Available at: http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews [Accessed 26 December 2011].

Cisco (2011) Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010–2015. Available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_pape r_c11-520862.html [Accessed 22 April 2011].

EC (European commission) (2008a) Towards a safer use of the internet for children in the EU – a parent‟s perspective, Analytic Report. [online] Available at: http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/analyticalreport_2008.pdf [Accessed 6 June 2011].

Finkelhor, D., Mitchell, K.J., and Wolak, J. (2008) *First Youth Internet Safety Survey (YISS-1)*, National Data Archive on Child Abuse and Neglect, Cornell University, Ithaca, New York.[online] Available at:http://www.ndacan.cornell.edu/NDACAN/Datasets/UserGuidePDFs/134user.pdf [Accessed 3June 2011].

Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011) *Final Report, LSE, London: EU Kids Online*. [online] Available at: http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx [Accessed 30 September 2011].

Livingstone, S., and Haddon, L. (2009) „Introduction‟ In: Livingstone, S. et al. (ed.), *Kids Online: Opportunities and risks for children*. Policy Press, Bristol: pp. 1-15.

Ofcom (2007) *Annex 2: Current tools and approaches to protecting children from harmful content online.* Available at: http://stakeholders.ofcom.org.uk/market-data-research/telecoms-research/byron/ [Accessed 23 December 2011].

SWGfL (2011) 360° Safe: *The self-review tool, South West Grid for Learning.* Available at: http://www.360safe.org.uk/ [Accessed 17 October 2011].