E-Safety and E-Security:
Raising security awareness among young people using peer education

S. Atkinson
Shirley.atkinson@plymouth.ac.uk

S.M. Furnell
s.furnell@plymouth.ac.uk

A.D. Phippen
Andy.phippen@plymouth.ac.uk

Centre for Information Security & Network Research, University of Plymouth, Plymouth, United Kingdom
cisnr@plymouth.ac.uk

Abstract
The potential for harm facilitated via Internet based behaviour presents modern society with a dilemma – on the one hand we wish to embrace new technology and the opportunities it affords. On the other, we wish to protect our families from the potential risks, in particular young people. However, many existing approaches use the risk laden environment as the foundation for the promotion of Internet awareness, which can incite parents and carers and lead to excessive measures for filtering and access. A more inclusive approach, which empowers young people to promote Internet awareness among their peers has been developed alongside a number of schools in the South West of the UK. Initial work with young people between the ages of 14 and 16 in these schools has allowed a good understanding of young people's attitudes toward online life, as well as demonstrating the potential of the peer led approach. However, the work has also highlighted a potentially detrimental effect of the e-Safety focus – while young people were clearly aware of the risks afforded with online behaviour, the more fundamental issues around Internet security were less well defined, with attitude and behaviour sometimes in conflict, demonstrating flaws in knowledge and the focus of Internet awareness in the young people's schooling.

Keywords: peer education, e-safety, safeguarding, e-security

Introduction
Home life has become more interconnected than ever. As reported by the Pew Internet Project (Kennedy, et al. 2008) the traditional nuclear family in America, with a married couple and children, now have the highest concentration of interconnected gadgets and communications devices. The pattern is similar within the UK and Europe, where the children are growing up with Web 2.0, the interactive web, while the adults in their lives are still struggling to understand its use (Staksrud, Livingstone and Haddon 2007). However, combine this growth in connectivity with attackers focusing on end-users of individual computers, rather than enterprise network attacks (social networking sites that are popular with children and young people providing access to confidential user information (Symantec 2008)) and a growing concern emerges about the darker side of the Internet.

Exploitation of end-users is facilitated by their online behaviours, where risk-taking often occurs with an apparent lack of concern about the potential for problems (Furnell, Tsaganidi and Phippen 2008). However, engaging with end-users to raise their awareness about safe behaviours online presents difficulties and requires a range of different education approaches. A particularly important aspect is considered to be the promotion of e-safe practices to children, as they will make first contact with IT services at an impressionable age and are enthusiastic adopters of new technologies. As such, they are recognised as being at significant risk if they are not equally aware of how to use it safely.

A number of initiatives already focus upon public awareness of e-safety and security, often with particular emphasis upon the protection of children online. For example, within the US, Wiredsafety.org (Wired Safety 2008) declares on the homepage that it is the world's largest Internet safety, help and education resource. The web page provides links to a variety of issues including Cyberbullying, online gaming safety and identity theft. Within the European Union, a €55M Safer Internet Programme will be launched on January 1st 2009 (European Union 2008) to follow on from an existing similar programme linking European organisations. In the UK, CEOP promote their ThinkUKnow programme within schools, aiming at parents and teachers with a series of hard hitting videos detailing their fight against child abusers (CEOP 2008).

Focussing on risks to young people requires a value judgement to be made, one which Furedi (2002) describes as allowing for manipulation of the fears of parents.

> "Virtual reality provides infinite space for the exercise of the anxious imagination, an unknown world where our fear of invisible strangers can run riot" (Furedi 2002).

The Byron Review (2007), commissioned by the UK Government, has been very influential in the UK for raising awareness about risks to children online, but started from the assumption of a risk-laden environment. As Sharples et al (2008) outline, this approach of concentrating on risks hampers helping young people to learn about safe and creative use of the Internet. Schools find it difficult to develop a policy of allowing young people access, due to pressure from parental and societal fears of abuse, preferring instead to filter and block.

In this context, the University of Plymouth has sought to investigate the attitudes of adolescents towards online safety and security, and to develop a peer-led approach to safer online behaviour. This paper presents the initial findings of that investigation, starting with an outline of the project before presenting focus group results. The paper discusses the results and concludes with suggested implications for online safety and security education programmes.

Method

Eight out of fifteen schools selected agreed to participate in the project. These were selected as being represented in the region in terms of gender balance and situation. Three schools were gender-specific and two had a religious character. One school was an independent day and boarding school, with the other five being general, non-denominational mixed schools.

Two schools shared the same specialist Maths and Computing status with the other six all having different specialist status.

The first phase of the project involved interviews with key school staff, followed by focus groups with the young people themselves. The initial semi-structured interviews explored the school approach to peer education and online safety, along with an overview of how they envisaged selecting young people to become e-safety ambassadors, and how they anticipated making use of the e-safety ambassadors within the school. .

During the time period from July to October 2008, a total of nine focus groups were held, collectively involving two hundred and two young people between the ages of fourteen and sixteen. With the exception of one school, the groups were held during normal ICT lessons and the participants were primarily young people that had chosen ICT as a subject at GCSE level (in the exception case the session was delivered to a group that had chosen to become peer-mentors within their school's existing peer mentoring programme).

The focus groups were designed to fill a normal school session of fifty-minutes and to be structured enough so that young people between the ages of fourteen and sixteen could remain engaged and participate. With this in mind, the focus groups incorporated a series of question and answer sessions (followed by discussion of issues arising from those questions so as not to skew the answers from the participants), interspersed with online searching and evaluating activities. The questions were designed to explore the participants' perceptions of online safety, to examine if and how they protected themselves online, and to consider their approaches to online security. The evaluation activities required them to critique four main UK internet safety websites.

- www.getsafeonline.co.uk
- www.internetsafetyzone.co.uk
- www.digizen.org
- www.thinkuknow.co.uk

Prior to all but two of the focus group sessions, a class list was obtained in advance, which was used to ascertain what information was publicly available about the children who would participate. Selected pictures and quotes from sources such as social networking profiles were then used in the presentations that seeded the discussions. Care was taken to balance potential for impact against the potential for distress, and montages of pictures and clusters of quotes were used to ensure that no individual was targeted. Pictures depicting risky behaviour were rejected in favour of group or individual photographs detailing happy occasions. No quotes were chosen that could have caused offence.

Following the focus groups, the participants were invited to become E-Safety Ambassadors and were invited to a launch day at the University of Plymouth in October 2008.

Interacting with pupils in a school setting is by no means straightforward for those outside of the immediate UK school environment. Access to pupils is regulated and therefore careful attention to ethical considerations had to be made. Each of the members of the research team had to have appropriate UK Criminal Record Bureau checks and the project as a whole had to be approved by the University Ethics Committee. As part of the ethical structure, forms were issued for parents to indicate their consent for the young person to participate were issued and briefing documents were made available to each school. Only two out of the eight schools made use of the parental consent forms, giving the students the option to not attend, whereas the other six deemed the session was an important part of the e-safety curriculum and that the young people were required to attend.

In addition to the ethical considerations, timing became very important. The target age range for the participants was between fourteen and sixteen. In the UK this is the period where they are working towards their GCSE examinations and therefore any interruptions to the lessons were not welcome. However, the design of the focus group session was welcomed as a learning tool for the ICT sessions and therefore facilitated the schools' engagement with the project. When making the appointments for the focus group sessions, two schools wished to hold their sessions in the July, post exam period and the rest of the schools opted to hold their sessions at the start of the new school year in September.

The number of participants in each session was primarily governed by the class size. One school had a large number of pupils decline to participate in the study, and therefore the focus group size ranged from eight to thirteen. In the other schools class sizes ranged from fifteen to thirty-two. Care was given to ensure that the discussions were not overly dominated by any particular individuals and to encourage all to contribute to the discussion or activity. The design of the focus group, along with\ session facilitation by the lead researcher, ensured that all the views could be gathered.

Findings and analysis

The class lists were used as one way of cross referencing the actions of the participants. The information gathered was used within the focus group itself. A total of 88 public social networking profiles were found, with the majority found on Bebo. One school proved an outstanding exception, their class list yielding no evidence of public profiles. Upon further investigation it emerged that this particular school had recently been engaging with the Plymouth City council Children's Services e-safety strategy (thereby demonstrating the effectiveness of the associated awareness-raising activity).

The public profiles led to 28 email addresses with an invitation to "add me" and 38 dates of birth. At the end of one of the focus groups, the participants were given the opportunity to adjust their privacy settings with continuing discussion around how to address privacy breaches arising from friends' profiles.

The montages of photographs and quotes triggered a shift in the level of engagement within the majority of the focus groups. In one of the groups, young people appeared bored and

restless in the initial stages, but upon being shown the results of a public search on their profiles they become attentive and engaged with comments emerging such as:

> "I thought my profile was private?"
>
> "That's me!"
>
> "Mine's private, but how did you get my picture?"
>
> "How did you get that photo?"
>
> "Privacy settings don't work!"

Perceptions

The focus group questions were designed to elucidate participant's perceptions of what threats were online and how they would deal with them.

When asked "were there any dangers on the Internet" each of the eight groups contained just one or two young people who demonstrated their knowledge of Internet threats such as viruses, Trojans and spyware and how they would deal with them. The others in the group appeared less confident in these areas yet all of them were enthusiastic in their suggestion that paedophiles were a threat. When discussing online risks and threats, Becta (Becta 2008) uses the following categories:

- Content – what is uploaded and downloaded.
- Commerce – scams, identity theft, and commercialism
- Contact – grooming, sexual and race hatred
- Culture – Cyberbullying and social networking.

However, on examining the responses when combined with rankings from these participants it became evident that a different framework to describe their terms would fit better:

- Cyberbullying
- Identity Frauds
- Internet Attacks
- Social Networking

The participants were invited to rank the dangers in terms of how they felt they might affect them personally. The ranking exercise was controlled in that only one vote for each of the three ranks were allowed for each person.

1. What was most likely to happen to you?
2. What could happen to you?

3. What was unlikely to happen to you?

Out of these values, those dangers related to Internet Attacks were perceived as the most likely, with Cyberbullying coming second and social networking issues coming a close third. Of least apparent concern were the issues surrounding identity frauds.

Internet Attacks
This category yielded the most elements of concern for the participants. Issues concerning viruses, spam, spyware, hacking, pornography and stumbling across inappropriate content were all raised. Spyware was considered the least likely problem with viruses and Trojans being the most likely. The breakdown of values is illustrated in Figure 1.

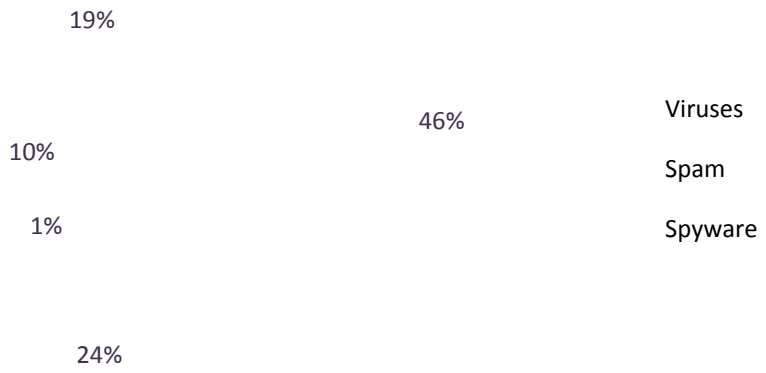

Figure 1: Breakdown of values for Internet Attacks

Cyberbullying
Within the context of Cyberbullying, four main areas arose. Cyberbullying itself was considered by the participants to be the most likely to happen them and this included the suggestions "bullying" and "bullying through Bebo". Sites that promoted hatred fell into this category, and these included gangs websites and hateful content that promoted bullying behaviour. Bullying and grooming behaviours from individuals were also included in this category. Unwanted contact was included in general terms and included wanted contact through the mobile phone. The breakdown of these values is illustrated in Figure 2

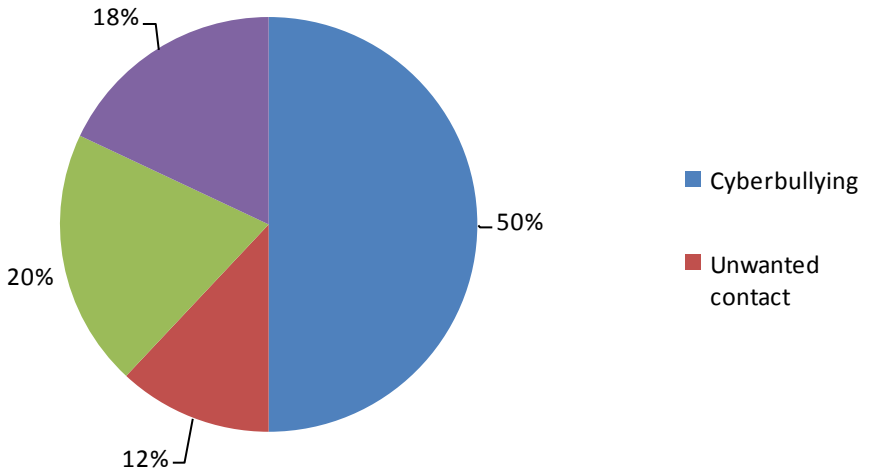

Figure 2: Breakdown of Cyberbullying values

Social Networking

The issues surrounding social networks primarily fell into three categories: Paedophile and grooming activity, personal information and the problem of hacked profiles. The primary concern was the potential for activity from paedophiles. Examples given within this category were arranging to meet, people not being who they said they were, paedophiles pretending to be teens. Whilst these dangers were the ones that captured the imagination the most, the values of perception illustrated in Figure 3of how likely they were to happen demonstrate that they were not considered to be the most likely to happen.

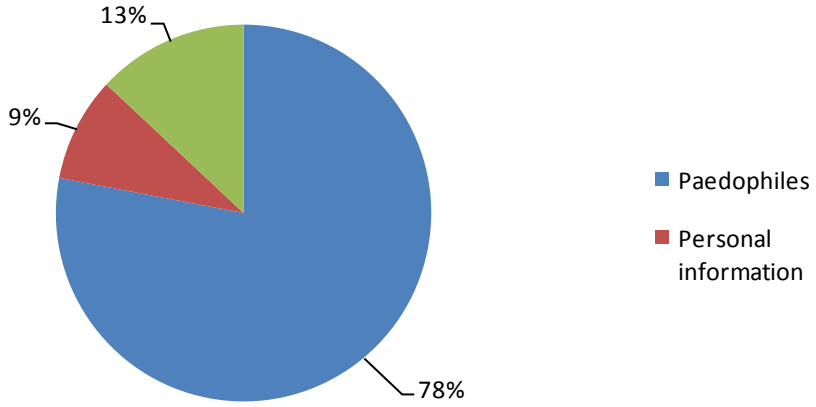

Figure 3: Breakdown of Social Networking values

Identity Fraud

This theme yielded the least suggestions and generated the least interaction from the participants, giving the impression that they did not view it as a problem. One group attributed their lack of interest in these areas to applying for credit, as they were not of an age

to do so; they consequently felt it was not an issue for them. In this category, the main concern emerged to be fraud and stealing of identity. The breakdown is given in Figure 4

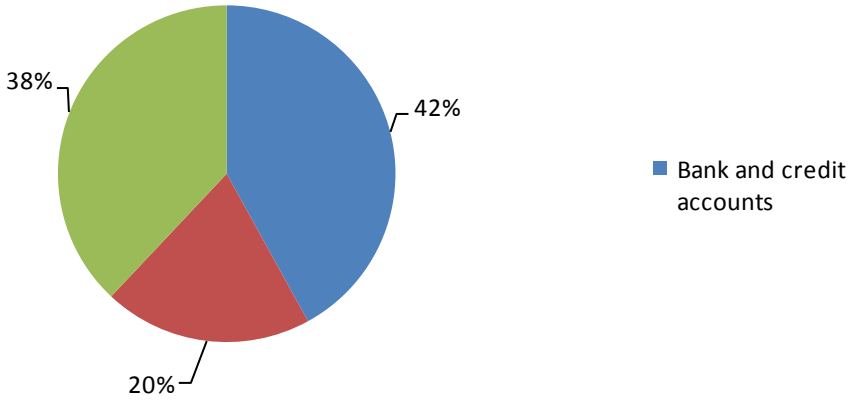

Figure 4: Breakdown of Internet Fraud values

When asked about who protects them, participants in four of the groups gave responses that indicated they were keen to leave it to other people. The most common responses involved individuals but responses tended to indicate that self-responsibility was not uppermost in their thoughts. Participants in all eight groups felt that family, friends and guardians were responsible for keeping them safe online – whereas only three of the groups suggested "self" should take responsibility. Suggestions that administrators and advisors were also responsible widened the circle of responsibility.

Approaches included:

- Factory settings
- Comes pre-installed
- The site protects my details.

Others favoured more software solutions with participants in five out of the eight groups giving specific named software for Anti-virus or Firewalls. Organisations were listed as being responsible, the most common being the school but included here was also the software companies and law enforcement bodies.

Safe Behaviour

During the discussions the participant's responses appeared to indicate that their behaviour erred on the side of keeping themselves safe. Examples of this were:

- Not opening attachments
- Reporting abusive behaviour online
- Using an alternative to Microsoft to avoid viruses

- Using strong passwords
- Not arranging to meet people they did not know
- Not accepting strangers on their online profiles

However, further discussion on strong passwords illustrated how they knew what this was, but only used strong passwords when they were forced to, in the case of Instant Messenger. In another discussion one participant was prepared to give her password to people if she trusted them:

> "If you give them your password like, you know, you've got to be careful who you choose. It's got to be somebody that you really trust before you can give it out. And like before, it's got to be somebody that you've known for ages. Like I'll give my sister it, and she likes want to go on it and she doesn't really care, and I don't know about my mates yet because, you don't really, I don't mind giving it to a couple of my friends who I really trust, but."

This was further illustrated by considering their public profiles and how they perceived this to be private even though the settings were not on private. Some defended this by saying that either the privacy settings did not work, or that they did not know how to make the privacy settings private. In one case, the naiveté of one individual was evident, one girl made clear her ambition was to be a model, therefore she felt her profile was there to publicise herself. However, during the ensuring discussion she determined that the link between herself, her school and her movements was one that could potentially put her at risk.

Conclusions

The focus groups have revealed some interesting findings in relation to how young people perceive the realm of online safety and security. For example, they were able to articulate the different types of threat that might affect them and were able to describe ways of keeping themselves safe.

Whilst the primary safety message articulated in each group was about the risk from online predators and unwanted contact, it was the Internet attacks which came out as the most likely. However, the related realms of safer online behaviour such as keeping passwords safe, is not as clearly embraced and there was evidence of the gap between what the young people were articulating and what their actions were.

This may perhaps emphasise the focus of the messages being delivered to this age range, for example we see the key messages with a child protection focus about risks online yet less with a security focus. This could be taken as an indication for further work required in this area, to engage with this age range further in a meaningful fashion.

Acknowledgements

The work described in this paper has been conducted with support from Becta, the British Educational Communications and Technology Agency.

References

Becta (2008) Mobile phones and Camera phones. http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_pp_mob_03 (accessed December 23, 2008).

Byron, T (2007) Safer Children in a Digital World. London: UK Government.

CEOP (2008) Child Exploitation and Online Protection Centre. December 2008. www.ceop.gov.uk (accessed December 22, 2008).

European Union (2008) Insafe Newsletter. December 2008. www.saferinternet.org/ww/en/pub/insafe/index.htm (accessed December 22, 2008).

Finkelhor, D & Jones, L (2008) Trends in Child Victimization. December 2008. www.unh.edu/ccrc/Trends/index.html (accessed December 22, 2008).

Furedi, F (2002) Paranoid Parenting. Chicago: Chicago Review Press Inc.

Furnell, S M, Tsaganidi, V & Phippen, AD (2008) "Security beliefs and barriers for novice Internet users." Computers and Security (Elsevier) 27: 235-240.

Kennedy, T. L.M. Smith, A, Wells, A.T & Wellman, B (2008) Networked Families. October 2008. www.pewinternet.org/PDF/r/266/report_display.asp (accessed December 22, 2008).

Sharples, M, Graber, R, Harrison, C, & Logan, K (2008) E-Safety and Web 2.0. Research Report, Becta.

Staksrud, E, Livingstone, S, & Haddon, L (2007) What Do We Know About Children's Use of Online Technologies? EC Safer Internet Plus Programme, London: EU Kids Online.

Symantec (2008) Symantec Internet Security Threat Report. Trends for June - December 2007. April 2008. www.symantec.com/business/theme.jsp?themeid=threatreport (accessed December 22, 2008).

Wired Safety (2008) Wired Safety. http://wiredsafety.org (accessed December 22, 2008).