Analysing the Extent that Children are Made Aware of Internet Security Issues Within UK Schools

B.A.Richardson and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
email: info@cscan.org

Abstract

Home computer users are increasingly becoming vulnerable to the threats of the Internet. One major reason for this is a lack of crucial security awareness amongst the older generation. Considering that children learn many life issues from their parents, the question has to be asked, how safe are their children? This paper presents results from a survey of 71 ICT school teachers about the teaching of security aspects in secondary schools; their awareness of the issues; and their views on responsibility and the National Curriculum. The findings reveal that there is a void in the curriculum with regards to computer security, which teachers are fully aware of. In addition, teachers lacked awareness of specific security issues resulting in an inadequate level of information being provided. There is a brief discussion about the current curriculum review regarding the proposed amendments and who it will affect. Moreover, suggestions are made as to whether the review is likely to be sufficient.

Keywords

Child protection, Teacher survey, Internet security, Security awareness, Curriculum review

1 Introduction

Home computer users are frequently exposed to dangers when using the Internet. As the commercial sector is tightening its own security, the home user is becoming more vulnerable. The number of home Internet connections is rising all the time with the vast majority (69%) being high speed broadband (National Statistics, 2007). With more and more homes installing fast Internet connections the home user is becoming an increasingly attractive target.

Home users make themselves vulnerable further by having a fairly low level of awareness of security concepts. Furthermore, home users are largely unaware that their actions (or inactions) impact greatly on other internet users. Many types of malware will propagate through the Internet infecting each vulnerable machine as it goes. With Sophos claiming that, “there is now a 50% chance of being infected by an Internet worm in just 12 minutes of being online using an unprotected, unpatched Windows PC” (Sophos, 2005), it is no wonder that unprotected home users fall foul to such attacks. Recent surveys have revealed that home users appear to be wise to some Internet security issues with the majority taking key protective measures; 83%

use anti-virus software and 78% have a firewall (Get Safe Online, 2006). Nevertheless, despite the high usage of such tools there still remains a poor level of security awareness on how to use them effectively.

One threat that has been rising for the last decade is phishing. This is defined as a "type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information" (Microsoft, 2006). In the first six months of 2007 Symantec discovered 196,860 unique phishing attempts and blocked 2.3 billion phishing messages (Symantec, 2007). A study revealed that 40% of people failed to spot phishing websites and 90% failed to spot the most realistic website (Dhamija, 2006).

Particularly vulnerable when using the Internet are children. In many cases they begin using the Internet from the age of 7 or 8, either introduced to it at home by their parents or at school during lessons which involve using computers. Children are particularly vulnerable because they are much more trusting and naïve to possible dangers. Many children use file sharing programs and technologies such as BitTorrent for downloading music and films illegally. Some problems that arise from using file sharing programs include opening up the user's computer to the Internet making them vulnerable to attack, and studies have revealed that 45% of executable files downloaded from such networks contain malicious code (Zetter, 2005).

In addition children can be prone to bullying; exposed to indecent images; and online grooming. Online grooming is described by the Child Exploitation and Online Protection Centre (CEOP) as "a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes" (CEOP, 2007a). Although it may be expected that this is a relatively minor threat, in reality on average 50,000 paedophiles are online at any one time (Goodchild and Owen, 2006), and 1 in 4 children have met in person someone they had only previously met on the Internet (CEOP, 2007b).

This paper examines the extent to which children are taught about Internet security issues at school through a survey of Information and Communication Technology (ICT) teachers. The main discussion begins with an outline of the survey's methodology and the demography of the respondent group. The teachers' awareness and knowledge of certain security issues is analysed followed by explanations of what issues they are required to teach their pupils about. The final part of the main discussion analyses the respondents' views with regards to responsibility and the current state of Internet security education. The paper concludes with a summary of the findings and a brief discussion on the future of ICT security within schools.

2 A survey of ICT school teachers

The study was undertaken during July 2007 and was delivered to ICT teachers via emails to their schools. The only criterion for respondents was that they taught ICT to children in at least one of the key stages[1] between 1 and 4 (ages 7-16). Six hundred UK primary and secondary school email addresses were gathered from local council websites, and requests for respondents were sent out to them.

The survey was hosted on a free website (securitysurvey.brinkster.net), and received a total of 71 responses. Please note that percentages presented in this paper are rounded, therefore some questions' results may not total exactly 100%. The majority of teachers were male (77%) and the average age was fairly high (45) as shown in Figure 1. Figure 2 illustrates that almost all of the respondents taught at a secondary school level (key stage 3 or 4), with only four teaching at either key stage one or two. Due to the limited number of primary school respondents, the survey findings presented here are based on secondary school teachers only.

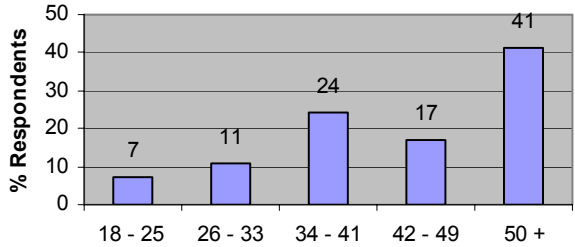

Figure 1: Respondents by age group

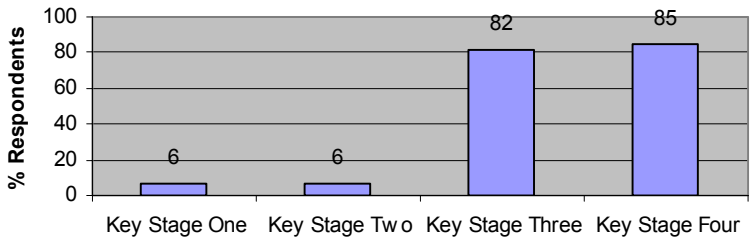

Figure 2: Respondents' teaching audience

[1] A key stage is a specific range of years of education in UK schools each ending with a formal assessment. Stages 1 and 2 form part of primary school (children aged 5-7 and 7-11). Stages 3 and 4 form part of secondary school (children aged 11-14 and 14-16).

The qualifications held by respondents were weighted towards Teaching Certificates (35%) and Degrees (49%), with a small number holding A-Levels (11%), one GCSE/O-Level and the remaining selecting other (3%). This included studying for a PHd and a post graduate degree. The spread of qualifications fit what was expected from a sample of ICT school teachers but with one surprising selection of GCSE/O-Level. This was unexpected considering the respondent taught at the same level as the highest qualification they held. However it could be the case that the respondent mistook the question for, "what level do you teach at?"

3 Awareness amongst teachers

The first section of the survey posed questions which would try to evaluate the respondents' knowledge about security issues, in order to understand the quality of the information they may give out to their pupils. Respondents were asked to state their level of awareness on a number of Internet threats as Figure 3 depicts. It is clear from the results of this question that the more recent threats are the ones that fewer respondents are aware of; botnets (19%) and pharming (12%). Surprisingly, around a tenth of ICT teachers do not know how to protect themselves against common threats such as Worms (9%), Trojan horses (10%) and spyware (8%).

The next stage of testing respondents' awareness of security issues was to give them six terms and six definitions which they were asked to match up. They were asked to pair up the terms file virus; macro virus; worm; Trojan horse; logic bomb; and botnet with the following definitions taken from BBC Webwise (2007):

- Malicious computer code that pretends to be a game or other interesting program that damages your PC as soon as you open it
- Waits and damages your computer when triggered by an event like a date
- Uses program files to get in and then copies itself
- A large number of compromised computers that are used to create and send spam or viruses or flood a network
- Infects your computer by using special codes found in word processing and spreadsheet files
- Does not damage files, but copies itself endlessly across computer networks and the Internet which slows them down

Not surprisingly, the correct definition for each term received the most responses. However, the number of incorrect answers was significant, given that the respondent sample consisted of ICT teachers. The threats that respondents previously claimed to be fully aware of received some of the lowest correct answers; file virus (64%), worm (36%), and Trojan horse (40%). Lesser known threats received middle of the range results; macro virus (87%), logic bomb (69%), and botnets (61%). The higher number of correct results for the less well known threats could be down to the fact that respondents were able to guess; this meant that some definitions could be easily assigned without any prior knowledge of the threat.

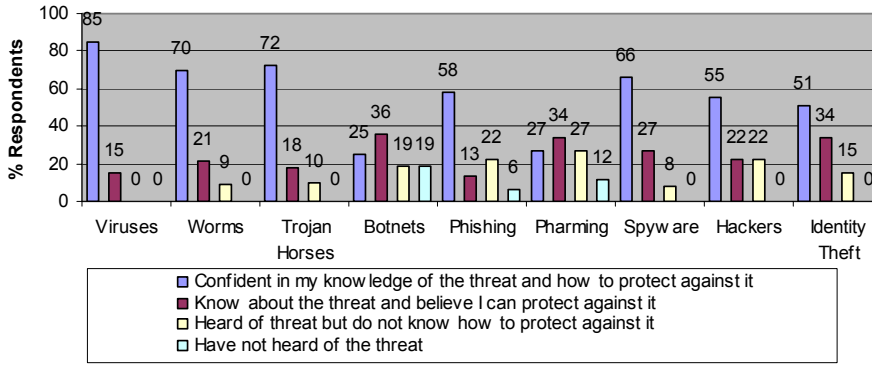

Figure 3: Respondents' awareness of Internet threats

The results from the awareness section of the survey were very worrying. It seemed that ICT professionals were unaware of key Internet threats and had false interpretations of ones that they were aware of.

4 Teaching practices

The second section of the teacher survey endeavoured to find out which security topics are taught in schools - respondents were asked to choose from a list of Internet security terms. As Figure 4 illustrates, the most common requirements (81%) were teaching about viruses, anti-virus software and safe online practices. Surprisingly, worms, Trojan horses and botnets which are just as dangerous as viruses if not more, were only required to be taught by 13% of respondents. Alarmingly, only 27% of teachers claimed that they are required to teach about updating software to patch security flaws. Another interesting finding concerns identity theft and phishing. 67% claimed that they teach about identity theft yet only 27% teach about phishing (i.e. one of the largest problems associated with online identity theft). Likewise, 40% of respondents taught about spyware but only 13% about its removal. It seems peculiar that related topics which are important for Internet security are not being linked in the classroom.

Of those who selected that they were required to teach about phishing (27%), all claimed to use visual examples of fraudulent emails and fake websites to get the issue across. Likewise, the respondents that teach about safe online practices (81%) shared similar views on what should not be disclosed when using the Internet. All advised not to give out your address; telephone number; send pictures of yourself; or meet in person. The vast majority (91%) recommended not to disclose your name and 83% advised against giving out the name of your school. Ideally, none of the information mentioned should be disclosed on the Internet whether it be on forums, social networking websites, in chat rooms, or on instant messenger. Oddly enough, some teachers were not advising children to keep their name or the school they

attend secret. These two pieces of information can be enough for children to put themselves in serious danger.

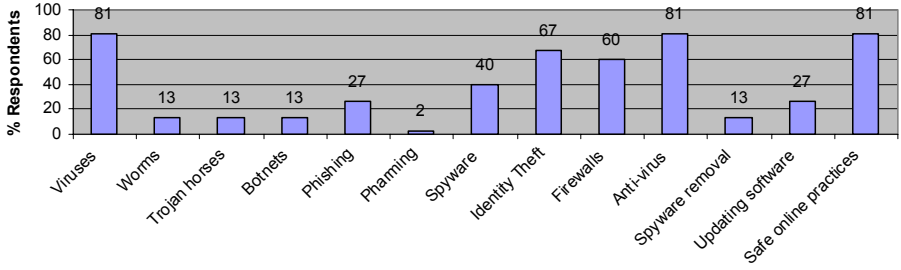

Figure 4: Respondents' teaching requirements

Those who taught about anti-virus software (81%) had a diverse view on updating virus definitions. As anti-virus software can only protect against viruses it knows about, and as new strains of malware are released every day, the only way to ensure maximum protection is to update the software as soon as an update becomes available. All reputable companies will release new virus definitions at least once a day. However as Figure 5 shows, only half of respondents advised updating this frequently. Thankfully, most of the remaining respondents (41% in all) selected once a week which should be the absolute minimum. Worryingly, 9% of ICT school teachers felt that updating anti-virus software once a month was sufficient to protect them from attack.

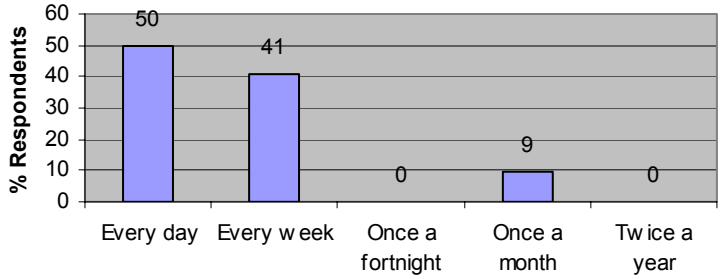

Figure 5: Respondents' recommendations for updating anti-virus software

Respondents were asked which websites they recommend to their pupils for receiving further information on Internet security issues. Amazingly, even with the apparent gaps in teaching security awareness, 57% of ICT teachers do not recommend any computer security information websites. The websites that are recommended by the remaining respondents are BBC Webwise (41%); Get Safe Online (9%); IT Safe (2%); and Wise Kids (2%). Note that the totals for this question total more than 100 percent as respondents were able to select more than one website. It is highly surprising considering the low level of security education being given that most teachers would not recommend any information websites to their

pupils. However, the failure to inform children of available help may be down to a lack of awareness that such websites exist.

Website	Visited	Aware of but not visited	Unaware of
BBC Webwise	54%	39%	8%
Get Safe Online	34%	0%	66%
IT Safe	13%	27%	60%

Table 1: Respondents' awareness of security information websites

Respondents were asked if they had heard of the major security information websites; table 1 shows their response. The majority of teachers had either not heard of them or did not know how informative they were as they had not visited them. The only website that was well known amongst respondents was BBC Webwise which only 8% had not heard of and 54% had actually visited. Government funded websites, Get Safe Online and IT Safe, had poor awareness with a large number of teachers having not heard of them, 66% and 60% respectively.

5 Respondent views

The final section of the survey asked respondents for their views on Internet security and teaching responsibilities. The teachers were asked how security focused they feel the current ICT curriculum is. As Figure 6 shows, the majority of respondents (48%) felt that there is very little focus on security issues with a further 13% believing that there is no focus at all. With that question in mind, respondents were asked if they teach additional information regarding Internet security which is not required of them under the curriculum; 46% agreed that they have taken it upon themselves to educate their pupils about particular threats. Some teachers explained that children receive additional information through an ICT Users Certificate that is taught at their school. Although a positive move to fill gaps in the curriculum, it is important to note that the majority of schools do not adopt this approach as they look to the curriculum for guidance on teaching.

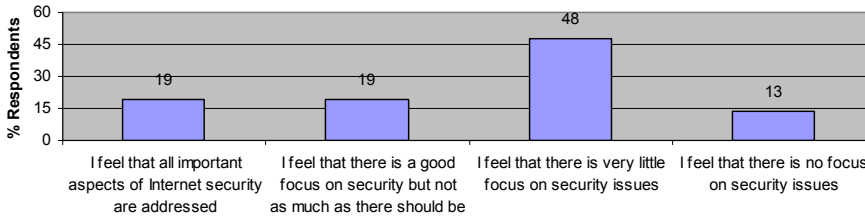

Figure 6: Respondents' views on the level of security focus in the curriculum

The final question of the survey asked respondents where they believe the primary responsibility lies in educating children about the threats of the Internet. Despite the fact that the survey has shown a low awareness amongst teachers and an inadequate coverage of the subject in the curriculum, the vast majority of teachers (70%) placed the responsibility with the schools. Almost all of the remaining respondents (25%) placed it with the parents. It seems extraordinary that so much expectation is placed on schools when next to nothing is actually delivered.

The respondents were asked if they had any further comments about the survey and the topic of Internet security. Below are two comments that sum up the situation within schools, with reference to educating children about the dangers of the Internet:

"The Key Stage 3 curriculum does not have a dedicated unit about security ... perhaps it should?"

"The National Curriculum and our exam spec (DiDA) do not require us to address these issues. We teach personal protection as part of our own take on duty of care, but so pushed for time to cover everything else that if it is not required we don't do it"

6 Curriculum review

The teacher survey has revealed a worrying lack of teaching about important security issues when using computers and the Internet. However, changes are on the horizon as an entire key stage 3 curriculum review is underway with key stage 4 in the pipeline. The changes are being made in all subjects to effectively update the National Curriculum (a framework that defines what children are taught in the UK), as it has not changed in around a decade. For subjects such as ICT this is extremely important as the rate of change is considerably higher than most other subjects (which tend to remain more consistent). Ideally, changes should be made to the ICT curriculum every few years to account for new technologies and threats. The new key stage 3 curriculum will roll out in September 2008 with key stage 4 the following year.

The current curriculum does not contain any security units and has no mention of security or protection at all. The most relevant reference made is in key stage 4 when pupils learn about the Data Protection Act 1998 and Computer Misuse 1990 Act. The revised key stage 3 curriculum will have a much larger focus on security with one of the key concepts being, "recognising issues of risk and safety surrounding the use of ICT" (QCA, 2007). The proposed syllabus also states that children will learn, "how to use ICT safely and responsibly … communicate and share information effectively, safely and responsibly" (QCA, 2007). They will also learn about "safe working practices in order to minimise physical stress" and "keeping information secure" (QCA, 2007).

The fact that the changes are only happening as part of an entire review of all subjects shows that the gravity of keeping children safe online has not yet been realised. The changes that are being made should help make a difference to the attitudes of children when using the Internet but how much is yet to be seen. One possible problem evident from the study is that many teachers are not fully aware of the issues. This means that unless they undergo training prior to the release of the new curriculum, they are likely to deliver inaccurate information which will only add to the problem.

7 Conclusions

This paper has examined a teacher survey, and has shown that there is a lack of education in schools about important security issues. Teachers openly admitted that there is very little focus on security in the secondary school curriculum although many of them made attempts to fill the gap of their own accord. The majority of teachers felt that schools are primarily responsible for educating children about Internet security issues, despite the fact that this is not currently the case. Many of the respondents lacked basic security knowledge that would be expected from an ICT teacher; the majority of respondents could not correctly identify the definition of a worm when presented with six very different answers. Perhaps most disappointing was that the majority of teachers did not advise pupils of any security information websites, even though they admitted that children do not receive enough on the subject at school. The survey has shown that there is a clear need for changes to be made to the curriculum, and that re-education of ICT teachers about old and new threats is required.

Thankfully, change is coming with the current review of the secondary curriculum. Security aspects are being added to key stage 3 to cover some of the basic issues. However, the quantity and quality of the delivery is yet to be examined as the new curriculum does not take effect until September 2008.

8 References

BBC Webwise (2007), “Online safety”, www.bbc.co.uk/webwise/course/safety/menu.shtml, (Accessed: 18 August 2007)

CEOP (2007a), “What is grooming and online child abuse?”, www.ceop.gov.uk/get_advice_what_is_grooming.html, (Accessed 18 August 2007)

CEOP (2007b), “Strategic Overview 2006-7”, www.ceop.gov.uk/pdfs/CEOPStrategicOverview2007.pdf, (Accessed 1 September 2007)

Dhamija (2006), “Why phishing works”, people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, (Accessed 7 September 2007)

Get Safe Online (2006), “The Get Safe Online Report 2006”, www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf, (Accessed 18 August 2007)

Goodchild, S. and Owen, J. (2006), "IoS investigation: Children & the Net", news.independent.co.uk/uk/politics/article1216003.ece, (Accessed 7 September 2007)

Microsoft (2006), “Recognize phishing scams and fraudulent e-mails”, www.microsoft.com/protect/yourself/phishing/identify.mspx, (Accessed 18 August 2007)

National Statistics (2007), “Internet Access”, www.statistics.gov.uk/cci/nugget.asp?id=8, (Accessed 18 August 2007)

QCA (2007), “The secondary curriculum review”, www.qca.org.uk/secondarycurriculumreview/subject/ks3/ict/index.htm, (Accessed 18 August 2007)

Sophos (2005), “Virus writing on the up as average time to infection spirals down”, www.sophos.com/pressoffice/news/articles/2005/07/pr_uk_midyearroundup2005.html, (Accessed 18 August 2007)

Symantec (2007), “Symantec Internet Security Threat Report: Trends for January – June 07”, eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf, (Accessed 17 September 2007)

Zetter, K. (2004), “KaZaA Delivers More Than Tunes”, Wired Magazine, January 2004