2006 - House of Lords enquiry into personal internet safety

This is UKERNA's submission to the House of Lords Select Committee on Science and Technology Sub-Committee investigation into Personal Internet Safety [1]. UKERNA is the non-profit company limited by guarantee that operates the JANET computer network connecting UK colleges, universities and research council establishments to each other and to the Internet and inter-connecting regional schools networks. Information about UKERNA is available on the website http://www.ja.net/ [2]

1. When private individuals connect their computers to the Internet they are entering a public space and are exposed to risks arising out of the nature of that space and the other computers and people who occupy it. As in real-world public spaces the level of risk to which an individual is exposed depends very much on how they behave. In recent years the nature of the most prevalent threats has changed, from technical attacks that target weaknesses in computers and software to 'social engineering' attacks that rely on lack of knowledge or careless behaviour by the user to succeed. Viruses, phishing attacks, on-line fraud and trojan horse programs are all examples of the latter type. Software vendors and Internet Service Providers continue to improve protection against technical threats: the greatest opportunity to improve personal internet safety is therefore to improve users' ability to avoid or resist social engineering attacks that exploit their human nature.

2. While it might be possible, to a limited extent, to impose Internet safety on users, this would inevitably require restrictions on what they can do and, in particular, make developing new services and ideas very much more difficult. Imposing safety (as is done, for example, when we travel by aeroplane) also makes users psychologically dependent on others for their safety and thus highly risk-averse and intolerant of any failure. The statistically illogical reaction of the public to rail and plane accidents, where safety is imposed, contrasts starkly with the response to the much higher, but apparently acceptable, rate of deaths in road accidents where individual drivers feel in control of their own safety. Any approach that attempts to impose safety on users of the Internet is likely to greatly limit the benefits that users, businesses and governments obtain from the network.

3. To achieve the full potential of the Internet as a tool that individuals are prepared to rely on for their daily lives – whether for e-commerce, e-banking, e-government, e-health or many other possibilities – it is therefore necessary to ensure that individuals know how to keep themselves safe on-line. Helping users understand that they can make themselves safer, and providing them with the knowledge and tools to do so, will not only improve their safety practice but also increase their confidence in using the Internet. A recent survey by the British Computer Society [3] found an increase in confidence among home users and attributed this to "a growing recognition of safe surfing and utilizing available tools to protect against threats". In a recent paper on social networking for young people, AoC Nilta state that "e-Safety education, not filtering and blocking, will

keep young people safe on line". A population that uses the Internet safely, has a stable confidence in it and does not suffer sudden changes of sentiment is essential if plans to provide private and public services over the Internet are to succeed.

4. The stable attitude and consistent behaviour of those users who feel in control may be contrasted with the situation where users rely on others, whether Government or service providers, to keep them safe. Ofcom's media literacy study [4] found large discrepancies between the fears expressed by parents and their actual behaviour: 72% of parents were concerned about their children seeing inappropriate things on line, yet only about half made use of content filtering services. Fear of on-line paedophiles is often expressed, but 40% of eight to eleven year olds use the Internet unsupervised and 23% of twelve to fifteen year old girls mostly use the Internet on their own in their bedrooms. Perception may be very different from actual risk. Concern about on-line "identity theft" is widespread but the BCS survey found only 8% of those surveyed had been a victim; in fact the vast majority of cases are simple credit card fraud which is at least as prevalent in the real world and where the individual's loss is limited by their contract with the issuer.

5. Advice in Internet safety and easy to use tools are already available but these need to be more widely promoted and adopted. For almost all personal computers tools such as automatic software updates, personal firewalls, anti-virus and anti-spyware are available either free or at low cost and can be used without specialist knowledge. Using these tools and checking advice sites such as Get Safe Online [5] and ITSafe [6] should be as routine as buying cars with safety devices, servicing them regularly and checking the weather forecast before using them. Demand from educated consumers for effective and usable Internet safety will also encourage and enable suppliers to further improve their products, establishing a virtuous spiral of improved safety.

6. Safe use of Information and Communications Technology can be taught, but it should also be demonstrated and applied whenever computers or networks are used. The Qualifications and Curriculum Authority's consultation on Key Skills [7] recognises the importance of these skills as a fundamental part of school education. All members of an information society need to know how to protect themselves and their personal information on-line (whether dealing with e-mail, websites or chatrooms), to assess the reliability of information and communications, to respect the personal and property rights of others and to use and maintain basic safety tools and behaviours. All opportunities to raise awareness, skill and confidence levels of users of all ages need to be taken – children who learn safe practice at school should be encouraged to teach their parents and grandparents at home. Childnet's Know It All for Parents [8] is an excellent example of how this can be done.

7. The confidence of Internet users will also be enhanced if they can see that those who misuse the network are held to account. Visible policing of the real world is now recognised as promoting citizens' feelings of safety. Unfortunately the policing of the Internet is much less apparent: the National High-Tech Crime Unit no longer publishes notices of successful prosecutions, regional police forces rarely have the resources to accept and investigate reports of Internet crimes and the Information Commissioner has publicly stated that his enforcement powers are ineffective.

8. Improving all individuals' ability and confidence to use the Internet safely is essential if society is to make effective use of this powerful communications medium. Unsafe users not only put themselves at risk, but are likely to make their computers and networks available for criminals to use to attack others. Addressing these problems requires citizens of all ages to know and practice Internet safety as naturally as road safety, cycling proficiency or motor car care.

Source URL: https://community-stg.jisc.ac.uk/library/consultations/2006-house-lords-enquiry-personal-internet-safety

Links
[1] http://www.parliament.uk/parliamentary_committees/lords_s_t_select/internet.cfm
[2] http://www.ja.net/
[3] http://www.bcs.org/server.php?show=ConWebDoc.6307
[4] http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/children/
[5] http://www.getsafeonline.org/
[6] http://www.itsafe.gov.uk/
[7] http://www.qca.org.uk/downloads/Functional_skills_draft_standards_for_consultation.pdf
[8] http://www.childnet-int.org/kia/