KEEPING KIDS SAFE ONLINE

By Zahri Yunos and Sharifah Sajidah Syed Noor Mohammad
National ICT Security and Emergency Response Centre (NISER)

(This article was published in NST – Computimes on 18 July 2005)

Children present additional challenges in terms of safety because of their natural characteristics: innocence, curiosity for new things, adventurers with little or no fear of punishment. We need to consider these characteristics when determining how to protect our children when they are online.

We may think that our children cannot cause any harm to us. What if they unintentionally visit pornographic websites? What if they unintentionally download computer viruses or worms?

Parents may monitor their children's surfing habits at home. In fact, what some parents do not realize that their children have also been accessing Internet at other places such as cybercafes and friends' home.

The Internet has been misused as a medium of child maltreatment as well as sexual and emotional abuse.[1] With unrestricted access, the tendency for young users to access pornographic material is very high, and once it's been seen, it would never be erased from their minds.

In an article entitled *One In Six Kids See Net Porn,* the author Amanda Hodge writes that one in six children as young as eight years old has been exposed to online pornography, frequently through pop-up advertisements.[2]

Children often imitate what they have seen, read, or heard. Studies suggest that exposure to pornography can drive kids to act out sexually against younger, smaller, and more vulnerable kids.

Apart from that, exposure to pornography is frequently results in sexual illnesses and sexual addiction. According to a study, as more and more children are exposed to softcore pornography and explicit deviant sexual material, they are pick-up extremely dangerous message. [3]

There were almost 400,000 attacks on Web sites around the world last year, a surge of 36 percent from 2003, according to a report issued by Internet watchdog agency Zone-H.[4]

On particular concern is the fact that the attacks on company and government Web sites spike during school holidays when the schoolchildren spend time in front of their computers rather than focus on their studies.

Hacking is a growing problem among the teenage community. From sometime now, computer hacking, software cracking, and Web site defacement have

gained the interest of teenagers. They look for excitement and do not understand the real implications of their actions.

The Milwaukee-based "414s" was one of the first teenage hacker groups whose members were arrested by the US Federal Bureau of Investigation in 1983 and convicted of breaking into more than 60 systems. [5]

In 1997, a Massachusetts teenager was charged with disabling the US Aviation Authority control tower for six hours at Worcester Regional Airport. [6] In June 2002, the Pentagon's computer networks were hacked by a 17-year-old teenager from Austria. He was reportedly successful in his attempt to obtain information on the location of military nuclear missiles. [7]

How can we make the Internet safe for young users and future generations?

Roles of parents. Parents have to take an active interest in their children's activities as well as full responsibility of preventing children from accessing offensive material on the Internet. Parents should implement responsible safeguards, ensuring that their children will have safe, educational and entertaining online experiences.

Parents also should closely monitor their children's activities online by placing the PC in an area of the home where they can easily monitor the children.

Parents may also try to establish online rules and an agreement with their children on the limitation of Internet use - of course with proper explanation.

Parents have to be alert of changes in their child's behavior. For example, a child who is secretive may indicate that he possesses inappropriate material or may have done something he knows is wrong.

Roles of service providers. It is essential for service providers / private organizations should also to offer assistance in disseminating information on safe Internet usage. They should also provide information on Web sites that are deemed unsuitable for children.

Service providers/private organizations should also conduct educational campaigns on Internet risks and safe surfing for children. As more and more sites offer offensive material, service providers/private organizations should develop software to filter or block access to these sites. In addition, online safety tips and information on filtering software should be made known to users.

Roles of Authorities. Obviously, there is an urgent need to conduct educational programmes on the nature and use of the Internet, including its inherent dangers. With the advancement of information communication technology (ICT), it is necessary to ensure that our education system is tailored to educating our children on safe computing.

This is important as our children would know the dos and don'ts when they are online.

Computer ethics might be introduced as a new subject in school. Ethics with regard to the use of ICT and data systems have to be addressed for primary and secondary schoolchildren.

Cybercafes have been used by youngsters to access undesirable sites and pursue activities such as Internet gambling and the viewing of pornography.

It is recommended that the Government makes it mandatory for cybercafe operators to install software to block access to pornographic and other excessive Web sites.

Cyber security is a shared responsibility of all - the Government, private and public sectors and the community. Within a relatively short period of time, the Internet has revolutionized communication and information sharing across the world, a revolution that has been eagerly embraced internationally.

Just as the Internet has become a source of significant positive change, it has also created new opportunities for the abuse or exploitation of children. With the growth of ICT and internet usage in Malaysia, it is crucial that safeguards be put in place now, rather than when it is too late.

REFERENCES

1. Feather, M., "Internet and Child Victimisation", Children and Crime: Victims and Offenders Conference, 17 - 18 June 1999**.** Brisbane: Australian Institute of Criminology. (http://www.aic.gov.au/conferences/children/feather)

2. Amanda Hodge, "One In Six Kids See Net Porn", The Australian IT, 23 April 2005. (http://australianit.news.com.au/australia)

3. Donna Rice Hughes, "Protecting Your Children In Cyberspace", Fleming H. Revell Company, 1 August 1998. (www.protectkids.com)

4. Roberto Preatoni, "Main Web Site Hackers are Schoolboys", Reuters.Know.How 25 April 2005. (http://www.zone-h.org)

5. Dan Verton, "The Hackers Diaries: Interview and Insight Into Teenager Hacking", McGraw-Hill/Osborne, April 2002 (http://www.osborne.com)

6. Frank J. Cilluffo, “Cyber Attack: The National Protection Plan and its Privacy Implications”, Homeland Security @ GW, 1 February 2001 **(**http://homelandsecurity.gwu.edu/congress**)**

7. “Komputer Pentagon Diceroboh”, Berita Harian, 16 Jun 2002