Teaching Children Cyber Security and Ethics

Cyber Security Industry Alliance

July 2005

Teaching Children Cyber Security and Ethics

CYBER SECURITY INDUSTRY ALLIANCE

JULY 2005

Reading, writing and arithmetic are the core of educational curricula for K-12, but there is great need to enhance this foundation by also teaching "cyber awareness" to all children. Cyber permeates most aspects of a modern child's life. It is a vital part of learning, playing, associating, socializing, and eventually working. Consequently, 99% of schools have PCs with access to the Internet.[1] The U.S. Census Bureau reports more than two thirds of households with children are more likely to have a PC.[2] In most metropolitan areas, nearly all households are connected to the Internet.

Contents

Children use PCs to learn traditional subjects, do homework and study, and for *edutainment.* As pervasive as edutainment has become, it is vital that America's children learn the ramifications that are possible through electronic commerce and transmissions. Email, instant messaging and text messaging connect them with friends, parents and other family, but they are also transforming the realms of stalking and predatory behavior. The Internet provides means for obtaining music, sharing digital photographs, playing games and blogging about personal life, yet no boundaries or legal borders are being placed on them at home or in school. These experiences are useful and important, but children need training in broader dimensions of cyber awareness in order to create a more educated, secure community as the information age sweeps through society. Cyber awareness education for children should include "survival skills" such as understanding spam, phishing, complications of chatting, wireless networking, and identity theft, to name a few. Just as we teach our children "right from wrong" in the physical world, we must ensure that the same lessons are taught in the cyber world as well.

[1] U.S. Department of Education, National Center for Education Statistics. (2003). *Internet Access in U.S. Public Schools and Classrooms: 1994-2002* (NCES 2004-011)
[2] U.S. Census Bureau, Current Population Survey, September 2001; Internet Release Date: November 19, 2004.

What is missing here is a focused and organized national effort to teach children cyber security, cyber ethics, and cyber safety with national security in mind. These elements of cyber awareness are vital because pervasive use of the Internet also poses risks that may harm the emotional and personal safety of children. The technology, unfortunately, enables devious and unethical behavior toward people, organizations or information technology underpinning critical infrastructure. The cyber education our children receive does not go far beyond how to turn on the computer and use a mouse. It is incomprehensible that we are not teaching cyber security, ethics, and safety at an early age. Poor awareness by children about cyber security may cause inadvertent damage to their own PC, other electronic devices or personal information, and could ultimately threaten the fabric of our nation's critical cyber infrastructure.

The Cyber Security Industry Alliance offers this briefing on the state of cyber awareness education for K-12 and offers policy considerations for Congress and the administration on teaching cyber security and ethics to our children. The briefing frames key problems, describes elements of cyber awareness, and provides snapshots of typical education programs for cyber security and ethics. While the focus of CSIA is on security, we have also included safety in this briefing for the sake of completeness. This briefing identifies whether the intended focus of a program's content is educators, parents or self-learning by children, and specifies if the funding sources are public, private or both. The briefing concludes with considerations for policy.

Members of the Cyber Security Industry Alliance fund several initiatives for teaching cyber security, ethics, and safety. Educational efforts such as this briefing are provided by CSIA as a public service.

PROBLEM SUMMARY

Many organizations are working on cyber awareness. Most efforts are private/public partnerships. Some programs are funded and operated by federal agencies, while others are for-profit commercial ventures. The key problem is that the myriad of programs for cyber security, ethics, and safety have no national coordination. Websites have substantial duplication of content; many of them seem to like what the others are doing, judging by an incestuous matrix of hot-links between their sites for "more information." There are no clear leaders, so there is no clear place for parents and teachers to learn what they must do.

President George W. Bush's *National Strategy to Secure Cyberspace* calls on individuals and industries to improve national security by securing the part of cyberspace they can influence or control. Cyber awareness for children is generally weak or missing in implementations of the national agenda. Quality education in core subjects has *No Child Left Behind.* Teaching children about the use and consequences of drugs has *Just Say No.* Parents who believe their child was abducted have *Amber Alert.* Cyber security, ethics, and safety have no such analog – yet.

Glossary

Cyber Security — Protecting a child's PC and personal information.

Cyber Ethics — Teaching children proper modes of behavior online.

Cyber Safety — Protecting children from unscrupulous people who initiate contact online.

WHO DOES THE TEACHING?

A key issue is the question of "Who does the teaching?" Some assume this kind of education should occur in school by teachers following authorized curricula. Perhaps it should. There is a need for guidelines and lesson plans to help teachers address cyber awareness as children use PCs and the Internet. But teachers' plates are already full with the challenging requirements of *No Child Left Behind.*

Adding sole responsibility to teachers for cyber awareness education could backfire. The national anti-drug message *Just Say No*, underpinned by the omnipresence of public service announcements, has produced a much more aware citizenry. In cyber awareness education, unlike in the anti-drug campaign, there has been no national effort to standardize expectations and methodologies for the teacher's role. A national cyber awareness program will provide the vital infrastructure for securing the country's technological-based fabric and develop awareness for future generations.

Parental involvement is critical to the success of any national canvass relating to our youth and would augment efforts made by teachers. Parents are responsible because they pay family Internet service fees for the PC, the mobile phone or PDA, instant messaging, digital music services and photo uploads. The parental responsibility for children's cyber awareness is fairly straightforward: parents should teach and enforce proper behavior.

TOO MANY WEB SITES

Too many web sites about cyber awareness are shouting for the attention of teachers, parents and children. The problem is not that there is too much information; the problem is that similar information appears in many places, keeping you wading through web pages, hotlinks and cross-links to other cyber awareness sites. Education on cyber awareness for teachers, parents, and especially children should not be so difficult to find. A few well-branded sites would be adequate and get would be faster and cheaper.

Many sites do not reflect the high quality we have come to expect from tier-one businesses, government, education, or non-profit sites. Organizational structure, governance and funding sources are often vague or incomplete. Copyright notices are years out of date. Pages are under construction. Hotlinks do not work. Some suggest "mom-and-pop" – a solo operation that got an initial burst of funding in the late 1990s or early 2000s and has since been in maintenance mode. These judgments may be harsh, but that is how people filter information on the web. If a site does not look professional, people may assume the content is not worth consideration. With a focused message provided by CSIA, both children and adults will develop more informed decisions about cyber use, act appropriately with cyber information, and safeguard personal information.

MULTIMEDIA IS BLASÉ

Americans live in a multimedia-intensive world, and our children have fully adopted every facet as an intrinsic part of our culture. The only multimedia that holds their attention is slick stuff produced by experts using sophisticated technology and content. For example, the 2004 $7.3 billion U.S. video game industry shows that American children are serious gamers. Budgets for high profile games ranging from $10 to $12 million provide rich content and enough focused attention to include advertisements within the games themselves. Presentation is everything with children; unfortunately, the general quality of cyber awareness multimedia is blasé. This may reflect the limited budgets of fragmented, uncoordinated education programs for children, a lack of national attention, or a general misunderstanding of the importance that should be associated with a national cyber education program. The quality of multimedia content must be impeccable when teaching cyber ethics to a child whose interests are hacking the school administrative mainframe or mastery of video reality games like *Grand Theft Auto.*

FUNDING IS UNCOORDINATED

In today's business and public budgetary climate, it is difficult to fund education efforts for cyber security, ethics, and safety. There is no coordinated effort for funding, so every organization must fend for itself. Fragmentation among the programs that win funding has impeded efforts to dramatically capture public attention, which means that the nation needs to pay more attention and spend more wisely. National coordination would help pool resources and radically boost the ability to produce quality curricula and multimedia required to train children.

Funding sources include federal and state governments, private and public corporations, charitable foundations, and parents. Federal funding often comes from agencies such as the Departments of Education, Homeland Security and Justice, and the National Science Foundation. A continued federal role is appropriate because risks posed by poor awareness of cyber security, ethics, and safety transcend state and national boundaries. Many risks originate in other countries.

TEACHING CYBER SECURITY

Cyber security entails teaching children about protection of their PC and their personal identity while using the Internet. Most of the responsibility for installation and maintenance of technical systems for cyber security appropriately rests with parents for home PCs and with education administrators for schools. However, children must be taught the consequences of actions such as widespread downloading of music, videos, graphics and other content from web sites that may be sources of viruses or software that infects their PC. Another simple action with potential for major damage is opening attachments to email from unknown senders – an action that can trigger cyber attacks on the initial PC and spread to many others over the Internet. Children also must be taught to restrict offering their personal information over the Internet.

Like cyber ethics and cyber safety, some web sites offer educators sample lesson plans, advice, resources and training on cyber security. Content often includes checklists, articles and links to other resources. Similar material is offered to parents and, more rarely, for self-learning by children.

Cyber Security Education **Typical Programs**	Teachers	Parents	Self-Learning	Public Funding	Private Funding
CERIAS – The Center for Education and Research on Information Assurance and Security at Purdue University provides information and programs for protecting critical computing and communications infrastructure. The K-12 Outreach Program aims to increase security of K-12 information systems, to integrate information security as a cross-curricular subject in K-12, and to raise parent and community awareness of IT security in K-12 schools. In addition to cyber security, CERIAS provides training materials for teaching cyber ethics and cyber safety. It has support from federal grants and more than a dozen commercial sponsors. www.cerias.purdue.edu/education/k-12	■	■		■	■
Consumer Information Security is a web portal by the U.S. Federal Trade Commission providing information for consumers about cyber security and safeguarding personal information. www.ftc.gov/bcp/conline/edcams/infosecurity/index.html	■	■	■	■	
CoSN – The Consortium for School Networking is a non-profit association that promotes the use of telecommunications to improve K-12 learning. Members include state departments of education, state networks, school districts, schools, individuals and companies committed to that goal. It's known for promoting adoption of the E-Rate program for schools and libraries. CoSN also lobbied against the Children's Internet Protection Act. Its Safeguarding the Wired Schoolhouse program provides advice for compliance with web content blocking and filtering requirements. http://securedistrict.cosn.org	■			■	■

Cyber Security Education **Typical Programs**	Teachers	Parents	Self-Learning	Public Funding	Private Funding
NCSA – The National Cyber Security Alliance is a resource for cyber security awareness and education for home users, small businesses, and schools, colleges and universities. A public-private partnership, NCSA sponsors include the Department of Homeland Security, Federal Trade Commission, and many private-sector corporations and organizations. NCSA provides tools and resources to empower users to stay safe online. Also offers the Top 10 Cyber Security Tips. **www.staysafeonline.org** or **www.staysafeonline.info**					

TEACHING CYBER ETHICS

Cyber ethics entails teaching children proper modes of behavior online. Children must be taught what behaviors are appropriate or inappropriate for interacting with other people online. Cyber ethics includes avoiding behavior such as hacking, writing or spreading viruses, stealing content and lying about its authorship by copying and pasting into a writing assignment, downloading copyrighted music or videos, copying CDs and software, or pulling online pranks such as smearing the reputation of another student. Some children may succumb to temptation because the Internet seems anonymous and free of the risk of being caught. Children also must be taught the legal consequences of inappropriate online behavior.

Like cyber safety, some web sites offer educators sample lesson plans, advice, resources and training on cyber safety. Content often includes checklists, articles and links to other resources. Similar material is offered to parents and for self-learning by children. Most self-learning games are appropriate only for a very young audience. A few sites offer games that teach cyber ethics and safety to various ages of children. The multimedia presentations suffer from the same general lack of sophistication found in products for cyber safety.

Cyber Ethics Education **Typical Programs**	Teachers	Parents	Self-Learning	Public Funding	Private Funding
Copyright Kids is a web site that teaches children the basics of copyright law. It includes quizzes, sample permission letters, directions on copyright registration and other links. The site was sponsored by the Copyright Society of U.S.A. www.copyrightkids.org					
Cyber Citizen Partnership Awareness Campaign provides information to teachers and parents for educating children and young adults on the dangers and consequences of cyber crime. It was created by a grant from the U.S. Dept. of Justice. Funding sources include private sector corporations, foundations and individuals. www.cybercitizenship.org					
Cyber Ethics for Kids is a free lesson plan and exercises teachers can use for children in K-8. It is provided by the U.S. Department of Justice. Objectives include teaching good cyber citizenship, rules in cyberspace, and consequences of hacking. www.cybercrime.gov/rules/kidinternet.htm					
Play It Cyber Safe by the Business Software Alliance provides curricula for teachers and parents, and online games for children for education about ethics issues such as inappropriate use of online content and software theft. One initiative is funded by Dept. of Justice in partnership with BSA and the Hamilton Fish Institute at George Washington University. www.playitcybersafe.com					

Cyber Ethics Education **Typical Programs**	Teachers	Parents	Self-Learning	Public Funding	Private Funding
Pro Music is a web site supporting legitimate use of music online. It provides teachers, parents and students with information about copyright laws for online music and dissuades illegal use of copyrighted material. The site is sponsored by the music industry and online services. http://www.pro-music.org/					
The Socrates Institute is an independent developer and evaluator of educational programs. Its CyberEthics Project for K-12 is developing classroom, video and web-based learning materials. The reality-style videos are of actual juvenile cybercrime case studies. A web-based role-play game educates children on responsibilities, safety measures, and legalities for using the Internet and other electronic data. Children also learn of the dangers and consequences of committing cybercrime. Funding support includes commercial, state and municipal providers. www.socratesinstitute.org					
U.S. Copyright Office site provides detailed information about copyright. www.copyright.gov					

TEACHING CYBER SAFETY

While the focus of CSIA is on cyber security, for the sake of completeness we have also summarized below cyber safety programs underway. For understandable reasons, cyber safety has received more attention and focus from government and education leaders than security and ethics. However, we encourage greater focus on the latter areas by policy makers as well.

Cyber safety entails teaching children how to protect themselves from unscrupulous people who operate web sites, contact them online, or attempt unsupervised meetings in person. Widespread opportunities for unsupervised use of the Internet demand that parents and teachers train children in cyber safety skills. Children must learn a healthy respect for the good and evil presented through a computer screen. Unlike the controllable, passive experience of television, Internet access presents real opportunities for luring children into unsafe situations, bullying or scaring them, and inflicting psychological or personal injury, abduction or death.

The U.S. Congress has encouraged schools to implement policies and protection technology to filter and block obscene content. The Children's Internet Protection Act of 2002 requires those steps to qualify for E-rate discounts and certain federal funding. Some schools teach cyber safety, but not as part of any federal or state mandated curricula. Some web sites offer educators sample lesson plans, advice, resources and training on cyber safety. Content often includes lists, articles and links to other resources. Similar material is offered to parents and for self-learning by children. Most self-learning games are appropriate only for a very young audience. A few sites offer games that teach cyber safety to various ages of children. The presentation of games is usually well below the sophisticated animation seen on television, motion pictures and video games. Most content is free of charge. A common characteristic is the assumption that readers have lots of time to read through articles on a myriad of web sites.

Cyber Safety Education **Typical Programs**	Teachers	Parents	Self-Learning	Public Funding	Private Funding
CyberSmart! Education Company provides free K-8 curriculum and non-sequential lesson plans on cyber safety, cyber ethics, and cyber security. It offers fee-based training for K-12 administrators, librarians, teachers and parents. Themes include safety, manners, advertising, research, and technology for online safety and information literacy. Cited online by NEA, American Federation of Teachers, Federal Trade Commission, Dept. of Justice, Dept. of Commerce, and state groups nationwide. Used in all 50 states and internationally. www.cybersmart.org	■	■			■
Get Net Wise is a portal of cyber safety and security information primarily for parents. It contains a useful summary of cognitive perspectives of Internet safety issues for children at different ages. The portal is produced by the non-profit Internet Education Foundation and funded by a wide range of private industry and public interest organizations. www.getnetwise.org		■			■

Cyber Safety Education Typical Programs	Teachers	Parents	Self-Learning	Public Funding	Private Funding
iSAFE is a non-profit Internet safety foundation bringing Internet safety education and awareness to K-12 students. It provides free curriculum to K-12 schools in all 50 states. Programs include teachers, parents and students. iSAFE also provides education in cyber ethics for children. Primary funding is from the U.S. Congress, with some corporate and individual sponsors. http://isafe.org					
NetSmartz Workshop is an interactive, educational safety resource that teaches children and teenagers how to be safe on the Internet. It includes resources for teachers and parents, and online games for children. The Workshop is primarily funded by the Dept. of Justice Office of Juvenile Justice and Delinquency Prevention and the Boys & Girls Clubs of America. Other partners include the National Center for Missing & Exploited Children, Hewlett-Packard, Cox Communications and Computer Associates. http://netsmartz.org					
A Parent's Guide to Internet Safety is published by the U.S. Federal Bureau of Investigation. It teaches parents how to help prevent the on-line exploitation of children. www.fbi.gov/publications/pguide/pguidee.htm					
Safe Kids is a web site to teach parents about online safety for their children. It is produced by Larry Magid, a syndicated columnist for the Los Angeles Times who is a long-time advocate for child safety online. www.safekids.com					
Safety Clicks! Is an initiative by America Online and the National School Boards Foundation. Web-based interactive games educate young children about online safety. The site includes other information for teachers and parents. www.safetyclicks.com					
Wired Kids says it is the world's largest online safety and help organization. More than 10,000 volunteers provide help. Web sites include information for parents and games for children. It's noted for work in Internet-related stalking, bullying, child pornography, identity theft, scams and fraud, and missing children. www.wiredkids.org					

CONSIDERATIONS FOR POLICY

While the Congress and Administration have committed some resources to cyber safety, we believe it is equally as important to focus on cyber security and ethics. CSIA urges Members of Congress and the Administration to consider the following policy recommendations for teaching cyber security and ethics to children in K-12.

1 – Create a national Cyber Awareness Program

Initiate a national-level program for teaching children K-12 cyber security, ethics, and safety, coordinated by the Administration, in particular, the Department of Homeland Security (DHS) and the Department of Education (DOE). The Cyber Awareness Program (CAP) should leverage a partnership between teachers and parents, with funding sources in the public and private sectors, and leadership from DHS. CAP should be designed and implemented with an eye toward not overburdening existing responsibilities by teachers. Guidelines, curricula, lesson plans, checklists, articles, success stories, multimedia games and other age-appropriate resources for self-learners should be easy to find and use by all. Congress should work to ensure appropriate resources and oversight are in place for such programs.

The National Cyber Security Alliance (NCSA) portal may provide an entry point for this program. NCSA is a national public-private partnership with support from government agencies, private corporations and nonprofits. It provides cyber security and cyber ethics materials, as well as links for parents, children, and administrators on the NCSA website (www.staysafeonline.org).

2 – Coordinate CAP content on web sites

The Cyber Awareness Program should simplify the process of finding resources for teachers and parents. CSIA recommends using a few branded web sites to coordinate CAP content presentation and use. There should be no question by teachers or parents about where to find the information and education resources.

3 – Ensure development of top-grade multimedia

A priority for coordinated funding should be creation, production and use of top-grade multimedia. Gaming technologies that teach cyber security and ethics would be extremely powerful. The Administration and Congress should encourage gaming companies to provide programs as a public service to schools.

4 – Coordinate public and private funding for CAP

CSIA recommends that the Cyber Awareness Program be a public / private partnership with focused national oversight. Coordinated funding sources should include federal and state governments, private and public corporations, charitable foundations, and parents. By coordinating funding of CAP, programs will gain focus and more efficient use of resources. Coordination will also facilitate measurement of program effectiveness.

This coordinated national-level Cyber Awareness Program will help bring effective education of cyber security, ethics, and safety to our nation's children, and improve the general state of cyber security in the United States. CSIA believes that the National Cyber Security Alliance (NCSA) can serve a very useful role in coordinating K-12 activities, bringing greater focus to efforts in this area, along with support from the administration and Congress.

ABOUT THE CYBER SECURITY INDUSTRY ALLIANCE

The Cyber Security Industry Alliance is an advocacy group to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. Launched in February 2004, the CSIA is the only public policy and advocacy group comprised exclusively of security software, hardware and service vendors that is addressing key cyber security issues. Members include BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc., Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc., iPass, Inc., Juniper Networks, Inc., McAfee, Inc., PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation, Surety, Inc., Symantec Corporation, and TechGuard Security.

About The National Cyber Security Alliance

The National Cyber Security Alliance (NCSA) is the go-to resource for cyber security awareness and education for home user, small business, and education audiences. A public-private partnership, NCSA sponsors include the Department of Homeland Security, Federal Trade Commission, and many private-sector corporations and organizations. NCSA provides tools and resources to empower home users, small businesses, and schools, colleges and universities to stay safe online. For more information, and to see the Top 10 Cyber Security Tips, visit www.staysafeonline.info

Cyber Security Industry Alliance
2020 North 14th Street N.
Suite 750
Arlington, VA 22201
(703) 894-CSIA
www.csialliance.org