A whitepaper published by
The National Cyber Security Alliance
Authors: Mala Bawer & Jim Teicher
Executive Directors, CyberSmart!®

Anticipated release date: May 5, 2004

An Action Agenda for Securing the Nation's Digital Resources: Start in Kindergarten!

Executive Summary

This white paper establishes an action agenda for education — literally beginning in kindergarten — to provide our society with the essential skills required for secure and trusted computing.

We identify education as vital to the safe operation of our critical infrastructures, and essential to making cyberspace a secure and trusted place to learn, play, work, shop and conduct business.

This is a dangerous game

Almost every day, a new story breaks involving the spread of a malicious computer virus or worm, or a scheme to defraud consumers over the Internet. Sadly, the perpetrators don't always understand the extent of the damage that their actions can unleash. Likewise, the victims of these attacks could have protected themselves had they known some simple precautions.

In our consumer culture, people have come to see the computer as just another toy. A fast, glittery, expensive toy that allows them to shop, chat, surf, e-mail – and impress their friends.

It's literally plug-and-play. You don't even need an instruction manual to get started. In fact, there is no instruction manual teaching any ground rules for safe, appropriate and effective use.

The problem is that now that we're all networked, how you play the game affects everybody else.

What security experts already know

In survey after survey, computers security experts repeat the same thing: corporate employee education is the "make or break" factor in protecting corporate digital property. This same lesson must now be applied to society.

Where to start? With kids

Young people, the largest segment of Internet users in the United States, know more about computers and the Internet than adults do.[1],[2] At least they use technology a lot more.[3] But there are serious gaps in their knowledge.

The main way kids now get technology skills is peer-to-peer, the equivalent of learning about sex from the street. They need systematic instruction on how to use computers and the Internet securely, effectively and responsibly.

But most adults are in no position to lead the way. Commonplace security breaches are widespread among homes with broadband access to the Internet.[4] And when it comes to stealing and cheating online, most are no different than children. Neither group thinks it is wrong. [5],[6]

Starting right now, young people must be taught effective cyber skills from the moment they are first allowed to touch a mouse. Their parents and older siblings will be challenged to catch up with them.

What we as a nation must do

There is a legion – 54 million strong – of young people who can lead the nation in secure and trustworthy computing. Many will enter the high-tech enabled workforce during this decade. A national commitment to teaching cyber skills will "trickle up" from these techno-savvy young people to adults. Because of this trickle-up phenomenon, investment in cyber security education and Internet skills training will begin to pay off immediately.

A critical juncture

Breaches in cyber security are growing exponentially. The incidence of Internet security breaches was 100 times greater in 2002 than in 1992.[7] The economic damages associated with cyber crime are staggering.

Security professionals fear major cyber attacks on their companies. And, although independent hackers and disgruntled employees have been the typical perpetrators of cyber crime over the past five years, the possibility that our nation's computing resources could be hijacked by terrorists is a real and growing threat.

Using computers and the Internet wisely and effectively is a 21st century core competency that can and must be taught.

This white paper calls for a national commitment and coordinated action agenda to teach cyber skills to young people in order to build the social foundation and culture of secure computing in the 21st century.

This document is a starting point: action-focused conversations among the stakeholders must now begin.

A whitepaper published by
The National Cyber Security Alliance
Authors: Mala Bawer & Jim Teicher
Executive Directors, CyberSmart!®

A Critical Juncture

Cyber security breaches threaten children, families, businesses — and, possibly, our national security.

- An estimated 40 million young people in the U.S. spend significant amounts of time online.[8] Many of them, states the National Cyber Security Alliance report "Fast and Present Danger," leave the family computer wide open to outside intrusion.[9]

- According to research firm eMarketer, 75 percent of children believe it's okay to reveal private family information online in exchange for free gifts.[10]

- The anonymity and ubiquity of the Internet affords endless ways for perpetrators of cyber crime to find unwitting victims. Identity theft, for example, accounted for nearly $48 billion in losses to businesses over the past five years.

  More than 27 million Americans have been victims of identity theft during that period, and nearly 10 million of those fell victim in 2002 alone, according to the U.S. Federal Trade Commission.[11]

- Economic damage associated with just two malicious infections in 2001 – the original Code Red worm and Code Red II virus – was estimated at more than $2 billion by the research firm Computer Economics.[12] If a virus were to infect 10 million computers owned by home users, the economic impact could be staggering.

- Breaches in cyber security are growing exponentially. Two out of three security professionals believe the risk of a major cyber attack on their company is likely.[13]

- The CERT Coordination Center at Carnegie Mellon University, a major reporting center for Internet security problems, received 21,756 incident reports in 2000, and a whopping 114,855 reports during the first three quarters of 2003. According to CERT, the incidence of Internet security breaches was 100 times greater in 2002 than in 1992. [14]

- The FBI's Operation Cybersweep uncovered Internet fraud schemes that resulted in $100 million of losses for 125,000 victims in just two months in the fall of 2003. [15]

The economic damages associated with cyber crime are staggering:

- $48B in identity theft losses over the past 5 years
- $2B in damages by just two malicious viruses.

" …a few lines of code could ultimately wreak as much havoc as a handful of bombs."

Tom Ridge, Department of Homeland Security Secretary

- U.S. Department of Homeland Security Secretary Tom Ridge said:

"The sheer reality is that we rely on computers…A vast electronic nervous system operates much of our nation's physical infrastructure. Everything from electricity grids to banking transactions to telecommunications depends on secure, reliable cyber networks. These networks and the infrastructures they support present an attractive target for terrorists. They know, as do we, that a few lines of code could ultimately wreak as much havoc as a handful of bombs."16

What security experts already know: The weakest link in secure, trustworthy computing is the human being.

In survey after survey, computer security experts repeat the same thing: corporate employee education is the "make or break" factor in protecting their digital property.

Computer security professionals stress the importance of educating employees about security awareness.

The need for cyber security education must now be addressed society-wide.

- Large financial services and high-tech organizations reported to *Information Security Magazine* that "user awareness" has the biggest impact on cyber security.[17]

- The Business Software Alliance/Information Systems Security Association cites "Lack of employee awareness" as the most significant barrier in implementing a cyber security program among larger companies.[18]

- The FBI/Computer Security Institute 2003 "Computer Crime and Security Survey" revealed that 78 percent of computer security professionals detected employee abuse of Internet access privileges. " The 223 security professionals who elaborated on this employee abuse said their companies, collectively, lost $456 million within the last 12 months as a result.[19]

- Independent hackers and disgruntled employees have consistently remained the most likely source of cyber attacks for the past five years.[20] Most cyber crimes are "inside jobs."

- Employee negligence or abuse of data warehouses or systems is the top concern of 97 percent of IT security executives.[21]

- Ernst & Young concludes: "Employee awareness can make or break your investment in security technology and processes."[22]

- The META Group Research finds that "most organizations will fail to successfully secure their

technology environment… because of communication [gaps between security professionals and their employees]."[23]

Adults are in no position to lead the way.

The majority of the people in the workforce today did not grow up using the Internet, and received no instruction on technology use at school. Dazzling advances in technology, from the speed of microprocessors to the ubiquity of high-speed Internet access have not been matched by training of the human beings who use these tools.

The main way youth get their technology skills is largely from peer-to-peer, the equivalent of learning about sex from the street.

- A landmark study released by the National Cyber Security Alliance, a coalition of companies and government agencies, found that commonplace security breaches are widespread among homes with broadband access to the Internet.[24]
    - 97 percent of homes in which children have broadband access do not utilize filters or parental controls
    - 67 percent do not have appropriately-configured firewalls
    - 62 percent do not regularly update anti-virus software
    - And, despite these evident vulnerabilities, 86 percent of broadband Internet users keep sensitive information on their home computer.

- Adults readily purchase a home computer for the educational benefits.[25] But, they may not know how to use it appropriately themselves. For example, nearly all adults who download music don't think they're stealing.[26]

- Nearly two-thirds of youth and parents agree that children know more about the Internet than their parents do, according to research conducted by the Pew Research Center and surpass their parents when it comes to using new technologies. [27],[28] In fact, young people represent the largest segment of Internet users in the United States.[29]

Teachers are inadequately trained to utilize technology.

Numerous studies conclude that teachers are not sufficiently proficient in technology use to support student achievement.

- Research by the California Department of Education, for example, reveals that only 13 percent of California K-12

teachers consider themselves "proficient" at technology use. Their report finds that "most experts agree that computers will have little impact on students unless teachers become skilled in using computers to challenge students, deliver content and reinforce important concepts." [30]

- This tremendous gap in teacher training exists despite the fact that according to the Department of Education, 99 percent of public schools in the United States have access to the Internet, and 94 percent of public schools use a broadband connection.[31]

Young people's educational use of the Internet is largely unsupervised.

Even young people's educational use of the Internet is outside of school, outside of the direction of teachers.

- " For most part, students' educational use of the Internet occurs outside of the school day, outside of the school building, outside the direction of their teachers," according to the widely disseminated report "The Digital Disconnect: The Widening Gap Between Internet-Savvy Students and Their Schools." [32]

Minors, not adults, are primarily responsible for the online sexual solicitation of other children.

Call it terribly inappropriate behavior, or real threats to children's physical and emotional security —children themselves, not adults are primarily responsible for the online sexual solicitation of minors. But the money spent to prosecute adult perpetrators of sex crimes dwarfs the total of all money spent on Internet education for young people.

The money spent to prosecute adult perpetrators of sex crimes dwarfs the total of all money spend on Internet education for young people.

But it's minors sexually luring other minors that are the bulk of the problem.

- According to the Crimes Against Children Research Center, one out of five minors reported being sexually solicited online. Only 24 percent of online solicitations of children are known to come from adults 18 and older, and only 4 percent of all solicitors were known to be older than 25.[33]

- Nevertheless, young people under the age of 18 accounted for just 3 percent of the 2,577 arrests by law enforcement for Internet sex crimes against minors during the 12 months starting July 1, 2000.[34]

Complex social issues — such as the concept of property in cyberspace, and the rampant cheating using the Internet —are not well understood.

Business models and technological safeguards have yet to catch up with the havoc wrought by illegal downloading and file sharing of digital property. Internet plagiarism is a growing concern, threatening to decay the fundamental values of academic integrity.

So far, neither business models, technology, nor the "threat of getting caught" have substantially curtailed pirating or academic cheating. Nor has society formed a widespread ethical consensus on these issues.

- According to the Business Software Alliance, a software industry trade group, 39 percent of the world's software is pirated resulting in global dollar losses in 2002 of $13.8 billion. The U.S. alone represents a dollar loss of nearly $2 billion, the second highest after China. [35]

- The Recording Industry Association of America reports that the music industry loses about $4.2 billion annually to piracy worldwide.[36] In response, the RIAA is spearheading a massive legal crackdown, hoping to deter pirates from downloading music without paying artists or distributors.

- Businesses are rushing to devise and test new product distribution models and technologies to prevent piracy. A prime example is Apple Computer's i-tunes, an online digital jukebox where music tracks can be purchased and then legally downloaded for 99 cents each. Other companies are working feverishly to devise viable mechanisms to make digital property harder to pirate and redistribute.

- In a 2003 survey of 1,000 U.S. college and university students and 300 college and university educators, Ipsos.com, a public opinion research firm, found that students don't respect digital property as "real" unless it comes in a box.[37]

    - 89 percent of students who download commercial software do not always pay for it.
    - 2 out of 5 students who use P2P file sharing programs to download commercial software say they are using it more than ever.
    - Only a quarter of students say piracy is wrong.
    - Only 14 percent of students surveyed believe their

It's not "real" unless it's in a box.

Nearly all adults who download music don't think they're stealing.

Only ¼ of students say piracy is wrong.

So far, neither business models, technology, or the 'threat of getting caught" have substantially curtailed pirating or academic cheating.

University's policy concerning unlicensed software is effective.
    - Although a majority of professors and administrators support policies to prevent piracy, few communicate this to their students.

- Research conducted by The Center for Academic Integrity at Duke University produced disturbing results concerning student plagiarism.

  The Center reported that over half of almost 4500 high school students interviewed "admitted they have engaged in some level of plagiarism on written assignments using the Internet" and that "most students have concluded that 'cut & paste' plagiarism – using a sentence or two (or more) from different sources on the Internet and weaving this information together into a paper without appropriate citation – is not a serious issue."[38]

The Opportunity: Start Young

Young people can lead the nation in secure and trustworthy computing.

A national commitment to teach cyber skills will "trickle up" from these techno-savvy youth to adults reaching 125 million Americans.

In survey after survey, computers security experts repeat the same thing: corporate employee education is the "make or break" factor in protecting digital property. This same lesson must now be applied to society.

Where to Start? The kids

There is a legion – 54 million strong – of young people who can lead the nation in secure and trustworthy computing. Many will enter a high-tech enabled workforce during this decade.

The U.S. Department of Education counts 53.8 million children, K-12, in our nation's public and private schools.[39] Together, these students have at least 75 million parents or household caregivers.[40] A systematic program for teaching secure and trustworthy computing skills K-12, therefore, has the opportunity to "trickle up" and reach at least 125 million people. This is nearly the number of Americans -- 146 million – who currently use the Internet.[41]

Because of this trickle-up phenomenon, investment in cyber security education and Internet skills training will begin to pay off immediately.

In the past, cyber security has been the domain of computing professionals and law enforcement agencies.

Cyber security must now become everyone's responsibility.

Our current notion of cyber security must start in kindergarten.

In the past, cyber security has been the domain of computing professionals and law enforcement agencies. But with the mainstreaming of the Internet, cyber security is now a shared responsibility of adults and tech-savvy children alike.

At this juncture, young people must be taught effective cyber skills from the moment they are first allowed to touch a mouse. As soon as children enter kindergarten, they are capable of embracing age-appropriate, responsible computing practices Their parents and older siblings will be challenged to catch up with them.

Developing good habits young is essential to building a positive culture of cyber security.

Once habits are formed, they are difficult to break regardless of age. Whether the habit is weight control, fingernail biting or poor information security practices, it's better to mold positive behavior than to modify negative behavior. Research in youth crime prevention suggests that intervention with at-risk children at a very young age curbs the onset of delinquent behavior by up to 80 percent.[42] Hence, it's reasonable to infer transfer that positive cyber skills must be introduced at the youngest possible age.

"We all live mostly by habit," Graybiel [MIT Professor of Neuroscience] says. Establishing new habits is difficult, and old habits formidable to change.[43]

For adults, this means making it more convenient and easier to do 'the right thing' and making each adult an individual stake holder in the practice of cyber secure habits.

Young people and adults— together —play a vital role in cyber security.

Hackers can literally turn even a home computer into a 'zombie'. The Mydoom worm, detected in January 2004, was sent as a simple file attachment to unsuspecting computer users around the world. When the malicious Mydoom attachment was opened, the infected computer turned into a zombie and was instructed to send out still more copies of the worm. Together, the zombies then launched massive denial of service attacks, flooding targeted web sites with requests for access, overloading them and causing the targeted sites to crash. Sadly, the perpetrators don't always understand the extent of the damage that their actions can unleash. Likewise, the victims of these attacks could have protected themselves had they known some simple precautions.

What we as a nation must do

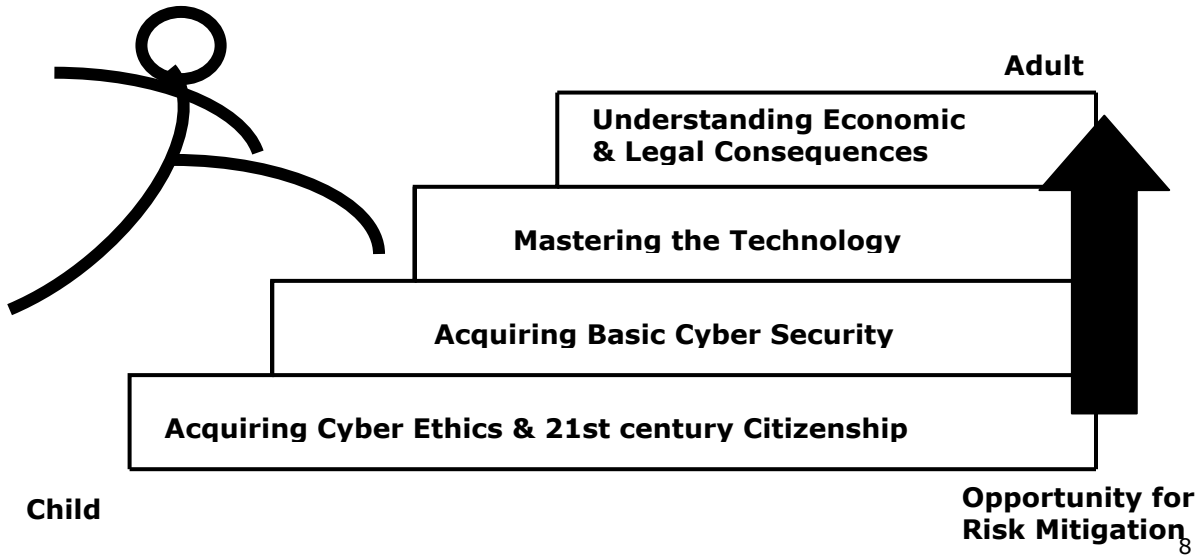
This white paper calls for a national commitment and coordinated action agenda to teach cyber skills to young people in order to build the social foundation and culture of secure computing in the 21st century.

Using the Internet wisely and effectively is a 21st century core competency that can and must be taught. Education is urgently needed to

- mitigate the risks of cyber security breaches
- protect our huge technology assets
- redress the havoc of stealing, cheating and crimes against children in cyberspace
- ensure that all citizens have the tools to participate fully in our democracy
- optimize the technology investments that schools have made over the past decade
- create a 21st century American workforce second to none.[44]

Mitigating Risks: Stepping up to Education

The chart below illustrates the components of teaching secure, responsible and effective use of comptuers and the Internet.



The steps to teaching and learning secure, responsible and effective computing practices include:

Acquiring cyber ethics and 21st century citizenship

> *"It is an axiom in my mind that our liberty can never be safe but in the hands of the people themselves, and that, too, of the people with a certain degree of instruction. This is the business of the state to effect, and on a general plan."*
> *Thomas Jefferson to George Washington 1786. ME: 19:24*

Jefferson viewed ethics, citizenship and literacy as core elements of an individual's ability to participate in self-government. If he were alive today, Jefferson would no doubt proclaim that all have their counterpart in cyberspace.

The need for teaching responsible citizenship is acknowledged in the mission statement of virtually every school district in the nation. For example, The Fairfax County, Virginia School District —one of the largest districts — affirms:

> *"The mission of the Fairfax County Public Schools is to educate all students to meet high academic standards and to prepare all students for responsible citizenship in the 21st century."* [45]

Americans need cyber skill training to effectively participate in our 21st century democracy.

The need for teaching responsible citizenship is acknowledged in the mission statement of virtually every school district in the nation.

Ethics and citizenship in cyberspace includes respect for digital property; an understanding of the special privileges and responsibilities of online communication; and the critical thinking and decision making skills to accountably manage one's actions in cyberspace.

The key concepts are:

- Respecting the contents of computers and networks
- Learning socially appropriate and acceptable behaviors for communication in cyberspace
- Exploring the implications of the Internet's open structure on a participatory democracy, including the negative possibilities of spreading false and hateful information

Acquiring basic security practices

We are not born with the skills necessary to function as effective 21st century citizens. The fact is, these essential skills must be learned:

- Safeguarding ourselves and protecting our private identify information in cyberspace
- Disconnecting a computer from the internet when not in use
- Learning to recognize online commercial intentions, including advertising, spam and various marketing schemes, which are often disguised as contests, opinion polls, warnings and personal messages.
- Understanding the laws pertaining to digital property and acceptable use of computer networks at home, at school and at the workplace
- Managing simple security practices like using hard-to-guess passwords, disconnecting from the Internet after an online session, and never opening an email from an unknown party
- Learning safe chatting and messaging skills

Mastering the technology

Learning simple precautions like disconnecting a computer from the internet when not in use and regularly updating anti-virus software can go a long way in securing computers and the Internet from virus attack.

Computer security practices that young people can bring home to their families include:

- Installing and updating anti-virus software
- Utilizing firewalls to protect the computer from Internet intruders
- Regularly downloading security-protection update patches
- Backing up computer data on a regular basis
- Understanding the risks associated with file sharing
- Preventing stranger access to private computer files

Practices that respond to the growing demands of information retrieval from vast amounts of data, ensuring participation in 21st century democracy include:

- Recognizing commercial or political intentions
- Evaluating the accuracy, relevance & comprehensiveness of online information resources
- Determining strategies for optimizing online research
- Utilizing search features to improve/refine research results
- Understanding the role of the librarian in navigating and selecting sources – particularly critical for young people where reading level and developmentally appropriate source material is required

Understanding Economic & Legal Consequences

Young people and adults alike need to understand the negative consequences and legal implications of irresponsible technology use. Our society relies on computers and computer networks, but these powerful systems – in the wrong hands - can also wreak havoc on corporations, individual citizens, our government and the economy.

The Stakeholders

A shared responsibility

The futurist Marshall McLuhan wrote that technology is an extension of the human body, and that the electronic media in particular are an extension of the nervous system. He did not live long enough to see how right he was.

Building a 21st century culture of responsible information sharing involves commitment & coordination among stakeholders

> *"The wheel…is an extension of the foot… the book…is an extension of the eye … Media, by altering the environment, evoke in us unique ratios of sense perceptions. The extension of any one sense alters the way we think and act – the way we perceive the world."*[46]

The technology of modern computing - the ability to manipulate data, engage in instant messaging, and reach millions of strangers with one keystroke – has literally rewired the human race.

The consequences of this rewiring are not yet known.

When cars were invented, nobody could have foreseen the elaborate social structures that this invention would ultimately spawn – driving schools, public classroom courses, licensing authorities, highway funds, traffic court and air pollution standards. It is obvious to us now that using cars safely requires the involvement of many players: industry, government, non-profit groups and the driving public.

So it is with computing. All the skills and habits connected with driving have analogies in the digital world. We must learn secure computing habits just as we have learned to secure our seatbelt. We need to navigate the digital highway safely – without causing harm to ourselves or others. And when we are finished, we need to secure our computers the way we secure our cars. Turning them off, locking them up (firewalls) and safeguarding our keys (passwords).

Building a 21st century culture of responsible information sharing involves the active participation of many stake holders. The public, industry, government, public/private partnerships, trade associations and non-profits.

Young people: learning to make secure computing choices

The process must begin with young people, whose habits are impressionable, and who are growing up with computers and the Internet.

Children must learn to make secure computing choices even when adults are not watching. As children mature, they begin to venture into public places on their own and take more responsibility for their own physical security. Similarly, as children age they make independent computing decisions based on a foundation of learned skills.

Learning developmentally appropriate ground rules for secure, responsible and effective technology use is a process. With the bulk of educational use of the Internet devoted to research, it is within the context of seeking information online — most often for social studies, but also for science, literacy and math — that issues of student safety, exposure to inappropriate material, advertising or inadequate source material habitually arise. Professionally developed lessons that are easily integrated into this process are required.

Daily, routine use of technology will increasingly require young adults to use— at various points during the day — the critical thinking and decision making skills needed for accountable cyber citizenship and acceptable, appropriate technology use. So too, should the student learning of these essential skills occur at various points during the school day.

These skills should include 'how to' on:

Safety: Using the Internet securely

- Protecting private identity information online
- Participating in chat forums safely
- Understanding the security implications of e-mail
- Recognizing uncomfortable feelings online and responsibly managing their actions

Manners: Understanding social, legal and ethical responsibilities

- Examining the power and responsibilities of cyber citizenship
- Respecting the law, including the digital property rights of others
- Learning to apply the same ethical principles in cyberspace that guide them in face-to-face situations
- Applying acceptable behaviors in cyberspace

Commerce: Identifying commercial messages & privacy protection

- Recognizing commercial/political intentions
- Recognizing online scams
- Understanding privacy policies
- Learning what it means to enter legal agreements when signing up for things online

Research: Using the Internet effectively

- Examining different strategies for research
- Evaluating the usefulness and appropriateness of informational Web sites
- Understanding the way the Internet facilitates our participatory democracy
- Recognizing the role of the librarian

Technology Practices: smart computing habits

- Safeguarding the family computer by installing firewalls, running virus software, choosing smart passwords and disconnecting from the Internet after a session
- Spreading safe computing practices to other members of the family who have not been explicitly trained

Parents: Bridging the digital divide

Learning and teaching cyber skills is an essential part of 21st-century parenting. Skills parents' need:

- Guidance on translating their basic values and good citizenship skills into cyberspace
- The basics of effective cyber security – from not opening suspicious e-mails to choosing appropriate passwords – and making these habits as automatic as locking the door
- Help in assessing the appropriate computer supervision/intervention their children need at varying ages
- How to evaluate the use of Internet filtering software and other tools to monitor children's online sessions
- Effective basic computing skills, including word processing, file management, installing software and online research

Educators: Laying the foundation for secure, effective trustworthy computing

Educators need to leverage their schools' enormous investment in educational technology. One goal of the No Child Left Behind Act of 2001 is to make every student in the country "technologically literate" by the end of 8th grade. Another is to fully integrate the use of technology into the academic curriculum.[47]

Just as it is hard to learn in a school that is not physically safe, it will be difficult to fully integrate technology into the curriculum unless the foundation has been laid to use that technology securely, responsibly and effectively. Teaching secure, responsible computing skills must become a mandated component of K-12 curriculum nationwide.

Teaching secure, responsible computing skills must become a mandated component of K-12 curriculum nationwide.

Early on, it appeared that Internet content filters would provide a technological solution to the problem of making sure young people were safe when they surfed the Internet. Although filters work at screening out objectionable content, they also screen out quality websites.[48] And filter programs do not prevent viruses, offer firewall protection or provide other security functions.

To mitigate liability and keep schools safe, teachers need to teach students how to react to any content or communication – no matter how offensive or objectionable – that they encounter online. Requiring students and parents to sign a computer network acceptable use policy (typically written in legalese and not at grade level comprehension) is insufficient.

Teachers require enough professional development training to allow them to smoothly integrate cyber effectiveness and security skills into their everyday administrative and teaching practices.

Librarians, too, are an essential part in securing the safe and effective use of computers and the Internet. Traditionally bridging barriers to information — including economic, linguistic diversity, usability/ disabilities, and geographic — librarians are now the navigators, or information specialists, to increasingly complex information retrieval.

Libraries and librarians have long played a "critical role in ensuring the full civic participation of a diverse population…supporting lifelong learning and supporting the democratic process." [49]

Industry: On-the-job education

Industry must work to build a strong culture of secure and responsible computing practices — to safeguard their business operations and leverage the Internet for growth.

Securing networks and expanding digital commerce have become common business practices. Industry has a huge stake in protecting this investment.

Industry must make its employees more aware of secure and responsible computing in order to:

- Protect digital property from theft and stem the growth of online piracy
- Protect corporate computers from unauthorized internal and external invasions
- Protect systems from malicious viruses and worms
- Safeguard the personal and financial information of clients
- Insure that consumers feel safe transacting business online
- Promote the growth of digital commerce

In addition to its own employees, industry has a stake in the public's level of computer literacy, responsibility and ethics:

- To groom high-tech workers for the future
- To develop a base of sophisticated and trustworthy customers
- To offset the need for a more stringent regulatory environment

Government: Homeland security and protecting commerce

A 30 % reduction in global software piracy would result in $64 billion in new taxes to help governments fund public programs like education, health care and law enforcement.

America's vast, interconnected networks of computers make us vulnerable to attack by those who wish us harm and who would undermine the democratic way of life. Sudden breakdowns in our nation's electric grid, telecommunications and broadcasting systems could lead to widespread chaos. The Blaster worm spread so quickly in January 2003 that within minutes systems ranging from the 9-1-1 telephone network in Seattle to the cellular phone service in Seoul had completely broken down. A more deliberate and systematic attack on our computers could bring our modern lifestyle literally to a halt.

The government also has a stake in protecting electronic commerce – both as the nation's largest buyer of goods and services and as the recipient of taxes generated by the sale of goods and services. According to the independent research firm IDC, a 30 percent reduction in global software piracy would result in $64 billion in new taxes to help governments fund public programs like education, health care and law enforcement.[50]

Just as the government tells citizens to be on the lookout for suspicious people and packages in airports and other crowded venues, it must train its citizenry to watch for suspicious events

online. The government must participate in funding cyber education and create strong partnerships with local, state and regional governments, industry and educational institutions.

It is also the government's role to provide deterrents to cyber-crime by rigorously prosecuting people who steal digital property or harm others online.

While being mindful of the risks to its citizens, the U.S. government must also create a regulatory environment that doesn't stifle innovation.

Trade associations and non-profits: spreading the word

Trade associations representing all industries – banking, securities, education, software and information industries, telecommunications, etc. – should educate their members about the need for cyber-security training, and provide it where appropriate.

By promoting education and self-regulation, trade groups and non-profit organizations can minimize the need for government regulation. The National Cyber Security Alliance, for example, is a cooperative effort between industry and government organizations to foster awareness of cyber security through educational outreach and public awareness. The Alliance provides cyber security tips and guides to security awareness, among other initiatives. InfraGuard, a partnership between private industry and the FBI, engages in cyber security education outreach at the local level.

The Return on Investment

Risk Mitigation
It is less expensive to educate technology users than to pay the costs associated with irresponsible computing. Young people are not born with the urge to commit cyber crimes or abuse the power afforded them by the Internet. Just as with other negative attitudes, these are learned behaviors. Education provides the opportunity to mitigate the risk of cyber security breaches.

By inculcating society with a culture of responsible cyber security behavior, teaching appropriate, acceptable use of technology and informing young people about the consequences of misusing computers and the Internet; education provides the foundation for effective risk mitigation.

For adults, who have not had this foundation, it will be necessary to provide continuous on the job training, reminders, and serious consequences for not obeying the law.

Investing in tomorrow's workforce

Education is an investment in tomorrow's workforce, prepared to face the challenges of the 21st century and in a safe and lawful Internet.

Education yields immediate results
Unlike investment in traditional education, which takes a full generation to pay off, investment in cyber security education will begin to pay off immediately. That's because, as we've said earlier in this white paper, technological know-how trickles up from more tech-savvy young people to their families, the workforce and society as a whole.

Improving academic achievement
A strong foundation in secure, responsible and effective technology use will enable schools to optimize their use of computers and the Internet to support academic achievement.

Promoting a cyber-secure America: The National Strategy

Our nation is now fully dependent on cyberspace for the operation of our critical infrastructure: transportation systems, electricity grids, the flow of money, and the various operations of government itself. "The National Strategy to Secure Cyber Space," U.S. Department of Homeland Security, is America's cyber security call to action, and enlists all citizens to secure our own piece of cyberspace. [51] Whether it be a home computer connected to the Internet or a large enterprise network, effective cyber security practices are essential, and new vulnerabilities require continuing response.

Education is a key element of the "National Strategy" document.

Action Agenda

- Federal, state and local governments must participate in funding for cyber security education programs, particularly those involving America's 50 million K-12 students.

- Industry, government and other interested parties must engage in coordinated public awareness campaigns that stress the value of the individual — both adult and young people — to communicate and share information responsible and securely online.

- The core group of industry trade associations and non-profits involved with promoting Internet education must expand. Now is the time to reach out to outlying trade groups to enlist broad-based industry support for cyber security education. Organizations representing securities, banking, health care, media, education and other industries all have significant roles to play.

- The hi-tech industry must implement practical cyber security technologies that combine ease-of use convenience, low cost to widespread deployment, and respect for privacy.

- Both the private sector and government should engage in research to determine the best information security educational practices.

- Schools must teach secure, responsible computing skills as part of a mandated K-12 curriculum nationwide.

- The U.S. Department of Education and states must prioritize teacher training for cyber skills, including information security, in order to effectively leverage technology in support of student achievement and preparation for the technology enabled workforce.

- The benefits associated with teacher training must be communicated to the senior education administrators who allocate and administer funds.

- The essential role of librarians as highly skilled navigators of an increasingly complex web of data sources must be acknowledged and support provided to librarians — in schools, universities and public and private settings —to strengthen the use of the Internet to sustain the integrity of academic achievement, life-long learning and the democratic processes.

About The National Cyber Security Alliance

The National Cyber Security Alliance is a unique partnership between the federal government, leading private sector companies, trade associations and non-profit groups. Their Web site staysafeoneline.info educates Americans on the need for computer security; encourages all computer users to protect their home and small business systems; provides a top ten list of tips, safety checklists, protective measures, and other tools promoting safe and responsible computer use.

About The Authors

Mala Bawer and Jim Teicher are founding members of The National Cyber Security Alliance. They co-direct CyberSmart! (www.cybersmart.org), a national leader teaching secure, responsible and effective Internet and computer use to K-12 students, educators, parents and enterprises.

Sources

[1] Bureau of the Census, *U.S. Department of Commerce*, September 2001.
[2] "Teens and Parents Survey, Pew Internet and American Life Project." *Pew Research Center*, December 2000.
[3] "Parents Online." *Pew Internet and American Life Project.* November 17,2002.
[4] "Fast and Present Danger: In-home Study on Broad Band Security Among American Consumers." *National Cyber Security Alliance*. June 2003.
[5] "Downloading Free Music: Internet Lovers Don't Think It's Stealing." *Pew Internet and American Life Project*, *Pew Research Center*, September 2000.
[6] "Internet Piracy on Campus." *Ipsos Public Affairs*. September 2003.
[7] *CERT/CC Statistics 1998-2003*. 20 January 2004 <http://www.cert.org/stats/cert stats.html>.
[8] Grunwald Associates, 2003.
[9] "Fast and Present Danger: In-home Study on Broad Band Security Among American Consumers." *National Cyber Security Alliance*. June 2003.
[10] "How Young People Spend." *EMarketer*. October 20, 2003.
[11] "Identity Theft Survey Report." *U.S. Federal Trade Commission*, September, 2003.
[12] "Malicious Code Attacks Had $13.2 Billion Economic Impact in 2001." *Computer Economics Press Release*. 4 January 2002. 20 January 2004 <http://www.computereconomics.com/article.cfm?id=133>

[13] "Information Security Study." *Business Software Alliance/Information Systems Security Association (BSA-ISSA)*. December 2003.
[14] *CERT/CC Statistics 1998-2003*. 20 January 2004 <http://www.cert.org/stats/cert stats.html>.
[15] Press Release, U.S. Department of Justice, 20 November 2003. 8 February 2004. <http://www.usdoj.gov/opa/pr/2003/November/03_crm_638.htm>.
[16] Remarks at the National Cyber Security Summit, San Jose, CA., December 3, 2003.
[17] "2002 Information Security Magazine Survey." *Information Security Magazine*.
[18] "Information Security Study." *BSA-ISSA.* December 3, 2003.
[19] "FBI/CSI Computer Crime and Security Survey." *Computer Security Institute.* 2003.
[20] "FBI/CSI Computer Crime and Security Survey." *Computer Security Institute.* 2003
[21] " 2003 Tracking Study on Information Security." *Unisys Corporation and Ponemon Institute*, October 2003.
[22] "Global Information Security Survey." *Ernst & Young*. 2002.
[23] "Security Program Effectiveness: META Group Research." META Group Press Release, 30 September 2003. 22 January 2004 <http://domino.metagroup.com/PressHome.nsf/(oldPressRelease)/B43EA65FE99AECA185256DB1006096CC?Open Document>.
[24] "Fast and Present Danger: In-home Study on Broad Band Security Among American Consumers." *National Cyber Security Alliance*. June 2003.
[25]" Key Technology Trends: Excerpts from New Research Findings." *Grunwald Associates*, June 2003.
[26] "Downloading Free Music: Internet Lovers Don't Think It's Stealing." *Pew Internet and American Life Project*, *Pew Research Center*, September 2000.
[27] "Teens and Parents Survey, Pew Internet and American Life Project." *Pew Research Center*, December 2000.
[28] "Parents Online." *Pew Internet and American Life Project.* November 17,2002.
[29] Bureau of the Census, *U.S. Department of Commerce*, September 2001.
[30] "Summary of Statewide Results from the 2001 California School Technology Survey." *California Department of Education*. September 2001.
[31] "Internet Access in U.S. Public Schools." *U.S. Department of Education*. Fall 2002.
[32] "The Digital Disconnect: the Widening Gap Between Internet Savvy Students and Their Schools." *Pew Internet & American Life Project* August 14, 2002. p.iii.
[33] "Online Victimization: A Report on the Nation's Youth." *Crimes Against Children Research Center*. June 2000.
[34] "Internet Sex Crimes Against Minors: The Response of Law Enforcement." *Crimes Against Children Research Center*. November 2003.

[35] "Global Software Piracy Study." *Business Software Alliance*, June 2003. 20 January 2004 <http://global.bsa.org/globalstudy/2003_GSPS.pdf >.
[36] Recording Industry Association of America. 20 January 2004 < http://www.riaa.com/issues/piracy/default.asp >.
[37] "Internet Piracy on Campus." *Ipsos Public Affairs*. September 2003.
[38] Center for Academic Integrity, Duke University 3 Februrary 2004 <http://www.academicintegrity.org/cai_research.asp>.
[39] "Projection of Education Statistics to 2012." *U.S. Department of Education National Center for Education Statistics.* August 2002.
[40] Census 2002, U.S. Census Bureau
[41] "Harris Poll #3." *Harris Interactive*. January 14, 2004
[42] "Less Hype, More Help: Reducing Juvenile Crime, What Works – And What Doesn't." *American Youth Policy Forum*, 2000.
[43] "MIT Researcher Explains Why New Year's Resolutions Don't Always Stick." *Science Daily*. 5 January 2000. 21 January 2004 <http://www.sciencedaily.com/releases/2000/01/000105051837.htm>.
[44] "Education and Training for the Information Technology Workforce." *U.S.Department of Commerce*. April 2003.
[45] "Mission Statement." *Fairfax County Public Schools*. January 20,2004 <http://www.fcps.edu/schlbd/targets.htm>.
[46] McLuhan/Fiore. *The Medium is the Massage*. New York: Bantam Books, Inc., 1967.
[47] Public Law 107-110, Part D.
[48] Digital Chaperones for Kids, *Consumer Reports,* March 2001.
[49] McCook, Kathleen. "Serving the Demands of Democracy: the critical role of libraries in ensuring the full civic participation of a diverse population." *Threshold, Exploring the Future of Educatio*n. *Cable in the Classroom*. Winter 2004.
[50]Expanding Global Economics: The Benefits of Reducing Software Piracy." *The Business Software Alliance,* April 2003.
[51] The National Strategy to Secure Cyberspace, The Whitehouse, February 2003.