Cyber-Safe Kids
Cyber-Savvy Teens
Cyber-Secure Schools

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Use of the Internet
Web sites: http://csriu.org
E-mail: nwillard@csriu.org

From Web 1.0 to 2.0

- Web 1.0 was largely one-directional
  - Web as information source
- Web 2.0 is participatory and mobile
  - All users can easily post information online and interact with others
  - From desk-top to personal digital devices
- Web 1.0 Internet safety strategies
  - How can we prevent children accessing inappropriate material and predators?
- Web 2.0 Internet protection strategies
  - How can we prepare young people to safety and responsibly contribute and collaborate in the online world?

Cyber Safe ~ Cyber Savvy

- When children are young, they should only use the Internet in safe places, with simple safety rules
- As they grow, they need the knowledge, skills, and values to independently make good choices online
- Adults need to remain "hands-on" to ensure they do

Outline of Presentation

- Part I. Overview and Insight
  - Overview of online safety risks and responsible use concerns
  - Web 1.0 strategies that are not working
  - Influences on youth online behavior
- Part II. Critical Issues for Schools
  - Typical concerns in schools
  - Effective Web 2.0 Internet use management strategies
  - Discussion Questions

Part I.

- Overview and Insight

Perspective

- Young people face risks online
  - And sometimes they do not make good choices
- Young people face risks in the Real World
  - And sometimes they do not make good choices

Range of Online Behavior

- Young people's online actions could be
- Innocent
- Risky
- Inappropriate
- Harmful
- Illegal

What Are the Risks?

Sexually Related Risks

- Pornography
  - Accidentally or intentionally accessing online pornography
- Sexual Activity
  - Grooming by adult predators to engage in sexual activities or provide pornography
  - Seeking sexual "hook-ups" with adults or other teens
- Sexual Harassment
  - Being victimized by or engaging in sexual harassment
- Displaying Sexual Material or Exploits
  - Posting or sending sexually provocative or explicit images
  - Discussing sexual exploits publicly

Cyberbullying

- Being cruel to others by sending or posting harmful material using the Internet or other digital technologies
  - Direct harassment
  - Denigration by posting hurtful materials
  - Impersonation to damage reputation
  - Making private embarrassing material public

Unsafe Online Communities

- Depressed teens becoming involved in self-harm "encouragement" communities
  - Suicide, cutting, anorexia, drug use, passing out, and the like
  - Already "at risk" youth find acceptance from like-minded peers
  - Can lead to contagion of unhealthy attitudes and behavior

Dangerous Online Groups

- Angry teens becoming involved in hate groups or gangs with adult members and recruiters or forming their own troublesome youth groups.
  - Already "at risk" youth find acceptance from like-minded peers or adults
  - Leads to contagion of unhealthy attitudes and behavior

Cyberthreats and Distress

- Posting online material that is a direct threat or raises concerns the person may be considering violence or self-harm
  - May be tied to involvement in unsafe community or dangerous group
  - Could be a joke, fantasy, unsubstantiated rumor, impersonation, or real threat!

Other Risks and Concerns

- Online Gaming
  - Excessive, addictive involvement in online games, some that are violent
- Online Gambling
  - Engaging in "gambling 101" game activities or actual online gambling
- Hacking
  - Breaking into or damaging computer systems
- Plagiarism
  - Inadvertently or intentionally using online information resources in an academically dishonest manner
- Copyright
  - Inappropriately copying, disseminating, or modifying someone copyrighted work
- Security Concerns
  - Accidentally infecting a computer with "malware"
  - Receiving excessive or highly inappropriate unwanted email messages
- Scams and Identity Theft
  - Being deceived by an online scam, including theft of financial identity information

Foundational Concerns

- Four foundational concerns underlie the specific risks
  - Unsafe Personal Disclosure
  - Addictive Access
  - Information Literacy
  - Stranger Safety

Unsafe Personal Disclosure

- Many teens appear to have limited understanding of potential harm or damage from inappropriate information disclosure
  - Are highly sensitive to any intrusion by parents or other responsible adults

Addictive Access

- Addictive access is an excessive amount of time spent using the Internet resulting in lack of healthy engagement in other areas of life

Information Literacy

- Anyone can post anything online
- People tend to judge accuracy of information based on appearance of the web site

Online Strangers

- Teens will have increasing engagement with online strangers
- Sometimes teens will want to meet in-person with an online stranger
- Most strangers are safe
  - But some are not

Activities and Technologies

- Social Networking
- Commercial Sites
- Chat Rooms and Groups
- Instant Messaging
- Cell Phones and PDAs

Social Networking Sites

- A place to express personal identity and maintain connections with friends
  - Create personal profile

  - Link with friends
  - Communicate
- Knowing how to effectively participate in this environment is **essential** for careers, personal life activities, and civic engagement in the 21st Century
- Concerns
  - Disclose personal contact, provocative, intimate or reputation damaging material
  - Unsafe connections with dangerous individuals or groups
  - Engage in or are targeted by cyberbullying
  - Addictive access
  - Lie about their age to participate

Commercial Sites

- Concerns
  - Market profiling
    - Encourage disclosure of personal information
  - Advertising
    - Promote unhealthy consumption, lifestyle, values, and behavior
  - Stickiness
    - Use specific strategies to encourage addictive access
- Online marketing techniques
  - Advergaming
    - Integrate advertisements into games or other entertainment
  - Permission marketing
    - Encourage youth to sign up to receive advertisements
  - Viral marketing
    - Encourage youth to send marketing material to peers

Other Activities/Technology

- Chat Rooms and Groups
  - Opportunity to communicate with others
    - Places where teens are most likely to meet unsafe online strangers
- Instant Messaging
  - Real time electronic communications using text or web cams
    - Strangers can be included on "buddy" list
    - Inappropriate material may be disseminated
- Cell Phones and PDAs
  - Mobile technologies limit the ability of adults to effectively supervise youth activities, especially in school

What is Not Working

- Fear-based tactics
- Reliance on filtering
- Simplistic rules
- Reliance on adults
- Uncomfortable information
- Child as victim

Fear-Based Tactics

- "One in seven youth has been sexually solicited online!!!"
- "If you provide personal information, a stranger will use this information to track you down and harm you"

Fear-Based Reality

- Research has shown
  - No relationship between providing personal information online and receiving sexual solicitations
  - Teens who meet with sexual predators do so knowing they are adults and intending to engage in sex
- "Sexual solicitation" included receiving unwanted sexual messages
- 43% of solicitors were younger than 18
  - Only 9% over 25
- 99% of incidents resolved by
  - Removing self from situation by blocking person or changing username or address
  - Telling person to stop
  - Ignored or didn't do anything
- Only in 1% of incidents police were called
- "Stranger-danger" warnings and fear-based prevention approaches are not effective
- The vast majority of online strangers are perfectly safe
  - Children and teens know this

Fear-Based Impact

- Teens know many adults do not understand the Internet
  - They dismiss fear-based message as evidence that adults fear what they do not understand
  - They are less willing to come to an adult for help ~ when they really should ~ because they think the adult will overreact!

Reliance on Filtering

- "Filtering technologies will protect young

people from harm as they surf the Internet"

Filtering Reality

- Will not effectively block "porn traps"
  - Because they link to new sites
- Will not deter determined teens
  - Because teens know how to jump fences
- Will not protect against risks related to online communication
- Is, at best, a "speed bump"

Filtering Reliance Impact

- Over reliance on fences has created a "false security" that children are protected and safe
- And the failure to …
  - Teach safety skills
  - Focus on responsible choices
  - Effectively monitor
  - Establish other limits

Simplistic Rules

- "Don't post personal information online"
- "Don't communicate with online strangers"
- "If you see something that makes you uncomfortable, tell an adult"

Youth Questions

- I use a username, so it is okay to post pictures of myself in a bikini. Right?
- How can I have fun on MySpace without sharing who I am?
- What if my new friend is a teen just like me?
- How would my mom know what to do?

Simplistic Rules Reality

- Simple safety rules are appropriate for children
- Tweens and teens must understand online risks and protective strategies to effectively prevent, detect and respond to the risks

Reliance on Adults

- "If you feel uncomfortable about something that happens online, tell an adult"

Reliance on Adults Reality

- Teens are not going to tell adults about online concerns if they think adults will …
  - Overreact
  - Blame them
  - Restrict their online access
  - Not know what to do
  - Make the problem worse!
- Which means we need to …
  - Do a better job of educating adults how to effectively respond to online concerns
  - Empower teens with the knowledge of effective responses, including actions to recommend to adults
  - Encourage competent teens to assist others

Uncomfortable Information

- Internet safety materials about sexual predators that does not
  - Use the word "sex"
  - Discuss sexual intentions of predators
  - Discuss provocative online actions that attract predators
  - Address why these relationships are unhealthy and dangerous

Uncomfortable Reality

- If adults are too scared to talk about risky sex with teens, then how do we expect teens will feel comfortable reporting to us that someone is "hitting on them" online?
  - We adults must openly discuss risky online sexual activities and predatory behavior
  - Before young people are participating in online environments where someone might "hit on them"

Child is Always the Victim

- "Understand, even if your child was a willing participant in any form of sexual exploitation, that he/she is not at fault and is the victim. The offender always bears the complete responsibility for his or her actions."
  - FBI A Parent's Guide to Internet Safety

Victim Reality

- The statement is legally accurate
- But teens are
  - Posting sexual provocative images
  - Using sexually inviting usernames
  - Trying to "hook up" online
- Teens are also engaging in
  - Cyberbullying
  - Unsafe communities
  - Dangerous groups
  - Hacking
  - Plagiarism
  - Copyright infringement

Safety and Responsible Use

- So it is also important to focus on how teens must be accountable for their online choices

Not-So-Good Choices

- Brain Development
- Disinhibition
- Exploration of Identity
- Emerging Sexuality
- Online Social Norms
- Social Influence
- Adolescent Risk

<u>"Didn't Think"</u>

- Brain Development
- Children do not have the cognitive development necessary to engage in safe online decision-making
- Teens' frontal cortex, which supports rational decision-making, is restructuring
  - Requires paying attention to actions and consequences

<u>You Can't See Me ~ I Can't See You</u>

- Disinhibition
- Perception of invisibility or creation of anonymity online …
  - Removes concerns of detection resulting in disapproval or punishment
- Lack of tangible feedback about the consequences of actions online …
  - Interferes with empathy and recognition of harmful consequences

<u>Who Am I?</u>

- Exploration of Identity
- High social anxiety can fuel addictive access and bad attention-getting choices
  - Friendship links and communication activity are new measures of social status and self-worth
- Public exploration of identity can lead to disclosure of highly intimate or reputation damaging material

<u>Am I Hot?</u>

- Emerging Sexuality
- In a society where advertisers, entertainment, clothing companies promote provocative sexuality
- Some teens are
  - Posting provocative images
  - Exploring sexual relationships and issues online
  - Electronic material can become public

<u>Everybody Does It</u>

- Online Social Norms
- "Life online is just a game"
- "It's not me ~ it's my online persona"
- "What happens online, stays online"
- "I have the free speech right to write or post anything I want regardless of the harm it might cause to another"
- "If I can do it, it must be okay"

<u>Doing What They Say</u>

- Social influence techniques
- Common online influence techniques
  - Provide gifts
  - Seek commitment
  - Encourage group allegiance
  - Create an attractive image
  - Establish a image of authority
  - Threaten loss to encourage action

<u>Looking for Love</u>

- Adolescent Risk
- Youth online risk must be viewed from perspective of adolescent risk
- Savvy ~ Naïve ~ Vulnerable ~ At Risk
- Savvy youth have effective knowledge, skills, and values to make good choices
  - Older experienced teens, healthy peer relationships, attentive parents
- Naïve youth lack sufficient knowledge and skills to effectively make good choices
  - Tweens and younger teens, may have over protective parents
  - Can become savvy with education and experience
- Vulnerable youth are going through a period of "teen angst"
  - Temporarily impaired relations with parents and/or peers
- "At risk" youth are those who are "at risk" in other areas of life
  - Face major ongoing challenges related to personal mental health and disruptions in relations with parents, school, and/or peers
- The greater the underlying risk, the more likely the youth will be …
  - Searching for acceptance and attention online
  - Vulnerable to manipulation
  - Emotionally upset, and thus less likely to make good choices because they are not "thinking clearly"

  - Less attentive to Internet safety messages
  - Less resilient in getting out of a difficult situation even if they want to
  - Less able or willing to rely on parents for assistance
  - Less likely to report an online dangerous situation to an adult because this will likely reveal evidence of their own unsafe or inappropriate choices

Web 2.0 Strategies

- Younger Children
- Tweens and Teens
- Vulnerable and At-Risk Youth

Younger Children

- For younger children, adults must be responsible for ensuring safety
  - Limited access to approved sites
  - Controlled communications
  - Simple rules
- Three simple rules
  - Don't go outside the safe places without an adult
  - Never type your name, address, or phone number.
  - If something "yucky" appears, turn off the monitor and tell an adult

Tweens and Teens

- What the risks are
- How to avoid risky situations
- How to detect if they are at risk
- How to respond effectively
- When to ask for help
- How to make good choices

Vulnerable and At Risk Youth

- Educate adults who are likely in the best position to detect and respond to concerns involving higher risk youth
- Develop effective teen "bystander strategies" to encourage competent teens to provide assistance to peers and report online concerns to adults

Part II

- Critical Issues for Schools

Continuous Improvement

- Technologies are changing
- New opportunities are emerging
- Greater insight into online risk
- Schools MUST engage in ongoing assessment, evaluation, and modification of technology implementation
  - Should be done without ascribing "fault" for past decisions

Typical Concerns in Schools

- "Internet recess"
- Monitoring and supervision
- Filtering
- Social networking technologies
- Personal digital devices

Internet Recess

- Student use of the Internet for non-educational activities
  - It is during "Internet recess" that misuse generally occurs
- Of special concern
  - 1:1 laptop programs
  - Substitutes
- Causes of "Internet recess"
  - Lack of standards for computer use
  - Lack of professional and curriculum development
  - Lack of technologies to create effective instructional activities
  - False security that filtering software is protecting students

Supervision and Monitoring

- Inadequate supervision and technical monitoring
- Causes
  - Lack of clear standards
  - Heavy investment by schools in filtering technology has restricted development and implementation of monitoring technologies
  - False security that filtering is effective

Filtering Concerns

Underblocking and Bypassing

- Filters will never effectively block all access to pornography
  - Especially "porn traps" because they link to newer sites
- Students can bypass the filter
  - Search "bypass Internet filter"
  - Generally they want to get to social networking sites, not pornography

Viewpoint Discrimination

- Filtering companies may engage in

unconstitutional viewpoint discrimination

- Filtering products include appropriate sites in categories with sites that are inappropriate

Interference with Instruction

- Curriculum review is an open process
  - With decisions made by educational professionals
- Internet blocking is not
  - Decisions made by filtering company are not based on instructional objectives
  - And are protected as "trade secrets"

Access for Safety

- Students are posting material online that is harming other students or providing evidence that they are at risk
- ALL SAFE SCHOOL PERSONNEL MUST HAVE THE ABILITY AND AUTHORITY TO IMMEDIATELY OVERRIDE THE FILTER!

Health and Well-being Sites

- Filters frequently block access to sites addressing sexual health and well-being issues
  - Often in categories with other sites that are entirely unacceptable
- But if students try to find such sites through a search engine, they may access entirely inappropriate material

No Ability to Rapidly Override

- The US Supreme Court upheld the Children's Internet Protection Act
  - Despite the proven problems of overblocking
  - Only because filters can be easily and rapidly overridden to allow access to inappropriately blocked sites
- But in many schools, no one has authority to override

Social Networking

- Social networking environments ARE the future of educational technology
  - Offer exciting opportunities to enrich student learning
  - Essential environments for preparation for work and life in the 21st Century
  - Opportunity to teach safety skills for these kinds of sites
- Present significant management concerns
- Commercial public sites are generally not appropriate for educational use
  - But may have intermittent educational value
- Maligned by fear-mongering

Personal Digital Devices

- Many schools have taught students how to use PDAs (handhelds)
- PDAs are increasing in capacity and decreasing in price
- Students will expect to use their own PDAs in the classroom for educational activities
- Concerns
  - Significant opportunity for misuse
  - No ability to filter
  - No ability to technically monitor
  - Less ability to supervise
  - Probably a violation of wiretapping laws to review electronic records on a student's PDA without parent consent

Cyber-Secure Schools

- Effective Coordination
- Educational Use
- Social Networking Environments
- Safer Environments
- Supervision and Monitoring
- Meaningful Consequences
- Internet Safety Education
- Accidental Access to Pornography
- Inappropriate Blocking
- Internet Concern Detection

Effective Coordination

- Schools MUST engage in ongoing assessment, evaluation, and modification of technology implementation
  - Regular solicitation of feedback from teachers and analysis of data
- Educational technology should be part of curriculum and instruction
  - Not technology services
- Addressing Internet safety and responsible use concerns must be coordinated by educational technology and safe school personnel
  - Educational technology personnel understand the technology issues
  - Safe school personnel understand youth risk
- When problems are identified, the initial response should be …
  - "How can we address this concern through better education, supervision, and

consequences?"

- Not simply blocking sites

Educational Use

- The better prepared teachers are to lead students in high quality exciting Internet-based learning activities, the more likely students will be on-task
  - When students are "on-task," problems dissipate
  - When students go to work, they will be expected to use their work computer for work activities only
- When students use the District Internet system, or their own PDAs in a classroom, such use must be for educational activities ONLY
  - Class assignments
  - Extra credit projects
  - High quality teacher-selected work-completion "reward" activities
  - Approved independent research
- Clear expectations
  - Whenever a teacher allows students to use computers, the teacher will be prepared with a lesson plan and extra credit or work completion activities
  - When students use the Internet in open labs, their use will be for classwork, extra credit projects, or approved independent research
- Supported by effective practices
  - Professional and curriculum development
  - Technology resources
    - Web page creation with white listing capability
    - Controlled communication and blog environments
  - Clear expectations for supervision and monitoring
  - Guidelines for open computer labs
  - Appropriate consequences for students and staff
  - Specific strategies for substitutes
  - Comprehensive plan for 1:1 laptops
  - Periodic review of usage data to assess whether the strategies are working

Social Networking

- Establish criteria for approved social networking environments
  - Support educational activities
  - Manage and monitor student use
  - Approved for consistent use
  - Override of filter for intermittent use of commercial sites
  - Watch out for strings attached to "free"

Safer Environments

- Elementary students should generally use the Internet in safe environments
  - Access generally limited to white-listed sites
  - Any open searching should be closely supervised and for a specific purpose
  - Well-monitored communications
- Youth health and well-being sites
  - District web page with access to reviewed sites providing quality medical and social information
  - Selected by health teachers, counselors, librarians, and medical/counseling associations
  - Medically accurate and appropriate for teens
    - Address information needs of sexually active teens and sexual orientation
  - If these sites are not in accord with a particular family's values, they can instruct their child not to access them

Supervision and Monitoring

- Clear expectation that Internet use by students will be supervised by staff
- Must create a high potential that misuse will be detected and lead to a meaningful consequence
  - Primary reliance on filtering must shift to better supervision and monitoring
- Effective supervision strategies
  - Placement of computers
  - Random, periodic request to see student history files (every 5 minutes)
  - Classroom aides, including student aides
- Expand use of technical monitoring
  - Real time remote access monitoring
  - Intelligent content analysis monitoring
- Significant concerns about effective monitoring with 1:1 laptop programs
  - Have not seen one report what students are spending time doing with computers
- Technical monitoring is essential

- After-school open labs preferable to take-home

Meaningful Consequences

- Misuse of the Internet must lead to a meaningful consequence
  - Suspension of all Internet access privileges frequently causes more work for teachers
- Requirement of service or extra-credit work project
- "Close monitoring status" for all Internet use
  - Easier to handle with a technical monitoring system
- Suspension of use in open labs or library

Accidental Access Happens

- No technology tool is infallible!
- Students or staff may accidentally access pornography
- ALL students and staff must know that if inappropriate material appears, they should quickly turn off the monitor or turn it so it can't be seen and report
- Responsible assessment of culpability
  - Students and staff deserve presumption of innocence and a fair investigation
  - This should be addressed in policy
- Fair investigation
  - Technical analysis to assess intention
    - Malware
    - Pattern of access
  - Assessment of circumstances
- Unless intent can be proven, assume accidental access

Appropriate Blocking

- Questions to ask …
  - Who has decided which sites/categories are blocked?
  - What is the educational basis of this decision?
  - How rapidly can the filter be overridden to support desired instructional activities or address safety concerns?
  - Who has (or should have) the authority and ability to override?
- Library media and curriculum staff should have primary authority for decisions related to selection of filtering categories to be blocked
  - They are the district's most highly trained professionals on issues related to the appropriateness of materials for students

Override Authority

- Selected staff in all school buildings must have authority and ability to quickly override the filter
  - All safe school personnel
  - Library media staff
  - Computer lab coordinators
- Temporary overrides are recorded, thus ensuring accountability

Internet Safety Education

- Students
- Parents
- Staff
- Lack of effective Web 2.0 Internet safety curriculum is a concern
  - Much of the current material is Web 1.0 based and incomplete

<u>Core Instruction</u>

- What the risks are
- How to avoid risky situations
- How to detect if they are at risk
- How to respond effectively
- When to ask for help
- How to make good choices

<u>Student Education</u>

- Simple rules for elementary students
- Introduce core principles in 5th grade after sex education
- Revisit core principles in middle school
- Focus in high school on preparation for adult use
- Direct instruction
  - Review of Internet use policy
  - Technology/library class
  - Health classes
- Teachable moments
  - Integrated into other instruction where appropriate
  - News stories

<u>Parents</u>

- Schools are an important conduit for information to parents
  - Parent workshops
  - Information in school newsletters
  - "Just in time" materials in office and counselor's room
  - Web 2.0 Internet safety books available in school library

<u>Professional Development</u>

- All educational staff
  - Effective Internet use management in schools
  - General knowledge of Internet risks and protection and intervention strategies
- Safe school staff
  - Comprehensive insight into youth risk online

Internet Concern Detection

- Students "connect" with different staff members
  - All staff members must have a good understanding of youth risk online concerns so that they can effectively respond if a student approaches them wanting to discuss an Internet concern
- Students are likely to start a conversation about Internet concerns with very subtle comments
  - Respond carefully, encouraging student to talk further
  - Discuss interaction with counselor, if perceive there might be a significant problem

Safe School Personnel

- Youth risk online must be viewed from the perspective of adolescent risk
  - All safe school personnel must have an excellent understanding of youth risk online issues

Discussion Questions

- How can your district/school more effectively engage in an ongoing, coordinated approach to address Internet use and safety issues?
  - What challenges do you face in addressing these issues?
- What specific Internet risk concerns are impacting your school community
  - What initiatives are necessary to address these concerns?

Closing Thoughts

- Cyberspace is our children's current and future world
- They are the "digital natives."
- At best, we adults are "digital immigrants."
  - And some adults are still in the "old country."
- Be we adults do have wisdom about making good choices
- And this is the wisdom that our children need from us