



# Protecting Children on the Internet

## July 28, 2006

Terry Gudaitis, PhD

## Discussion Topics

- What are Children Doing on the Internet?
- How are their behaviors putting them at risk?
- What are some of the “popular” recommendations...and why should some of them be changed?
- What should parents do?
- What can law enforcement do to assist parents and children?

## What are Kids Doing?

- Websites
- Blogs (static postings)  
EX: LiveJournal
- Social Networking Sites (auto-linking and cross-linking)  
EX: MySpace
- Chat (IRC)
- Message Boards
- Forums
- Text Messaging
- Gaming Sites

## What is putting Kids at Risk?

- Self-Disclosure of Demographics
- Self-Disclosure of Psychological or Emotional Needs
- Disclosure of Geographics
- Identification of Materialistic Wants
- Innocence and Naïveté
- Desire to Communicate in the “Global Environment”
- Desire for Affirmation

## Other Behaviors that place a child in a threatening, vulnerable, or risky position....What to do?

- Your child may not be disclosing information....but a “friend” posting a comment or message may be providing the identifying information
- The site itself may be based on technology that auto-links like information on your child’s site
- Other Adults who post or blog information about children (i.e., teachers, day-care centers, photographers, camp counselors...and, yes parents) – the intent is usually not malicious...but...
- Other children who are using other means of communication (video, photos) to post information to the Internet (i.e., YouTube.com, flickr.com)

## Popular Recommendations...that should not be so popular...

- **Restriction of Access**
  - \*Study – April 2005, London School of Economics – restriction can stifle education, success, and job opportunities.
  - \*Denying access is not a solution
- **Net-Blockers, Net-Nannies, Spyware, etc... are effective**
  - \*Only as long as it takes for the child to figure it out or have a peer teach him/her how to circumvent
  - \*Only as long as the technology is current
- **Keeping the computer in a “public area” will keep the child safe**
  - \*The child will conform to the rules while in eye-shot
  - \*The times of concern should be when the child is not in site (i.e., at school, at a friend’s home, at the library, at a cyber café) and good habits need to be enacted at all times

## Recommendations for Parents and Law Enforcement

- Parents **MUST** sign up for their own blog so they truly understand how they work – different sites use different underlying technologies.
- Parents **MUST** understand the basics of the Internet to have any credibility to dictate rules regarding Internet use to their kids – this includes the different search engines (i.e., text, blogs, images, videos, peoplefinders, bookmark searches – not just Google) and how to check the cache, Internet History files, and Temp files.
- Parents need to create parallel lessons and “plans” – tangible world to cyber world – and have the same steps:
  - Identification of Threat
  - Immediate Behavior
  - Follow-up Actions
  - ReportingEX: Talking to Strangers

## More Recommendations....

- Define and be very specific about the types of threats – each will need a slightly different plan and response:
  - CyberBullying
  - Solicitation
  - Harassment
  - Stalking
  - Spam
  - Identity Theft
  - Pornographic or Adult Content
- Have “would you put it on a Billboard on the highway” litmus test
- Be knowledgeable regarding miniature devices that can be easily installed and uninstalled or hidden (i.e., webcams, USB keys, capability of iPods)
- Establish rules and guidelines regarding Internet name usage as well as content management - Using an alias while still posting questionable content is still not safe...

## Just a Few More....

- Evaluate the security of the school's website and how electronic communication is allowed on school grounds.
- When the child is old enough – use “search games” as a learning tool to have the child find blogs, sites that he/she feels are “not secure” and have the child explain why
- Manners, etiquette...bad Internet behavior invites bad Internet behavior
- Content placed on the Internet cannot be erased and are not always “invisible” to those who are not granted access – some content is visible via indexing and search engine displays.
- Learn and understand some of the workarounds – free email accounts, encryption, anonymizers, anti-spyware detectors, steganography...
- And don't forget about the basics – Adware, content-blockers, anti-virus, spam-blockers, passwords (changing passwords), know the buddy lists and friends lists, etc...  
Many sites present lists of the “basics”

## Contact Information

Questions? Comments?

**Terry Gudaitis, PhD**

**Director, Open Source Intelligence**

**SAIC**

**[gudaitist@saic.com](mailto:gudaitist@saic.com)**