NCSA Cyber Security Education Roundtable Part I: The importance of "cyber security, safety and ethics education" for children and young adults in preparing them to be good cyber citizens

No Cyberchild Left Behind

Thank you for sharing your time with me this morning. The subject I want to discuss with you, which I refer to as C3, is Cyberethics, Cybersafety, and Cybersecurity in the K-12 educational arena. As our nation continues to build its cyberinfrastructure, it is equally important that we educate our population to work properly within this construct. Not only must they be good citizens from a fair use and "netiquette" perspective, but they must also know best practices in protecting their own data and system, as well as the network and systems on which they work. As in many cases, the best way to reach our citizenry is to teach them within the K-12 environment. Unfortunately, this process is woefully inadequate at present, although many new initiatives show promise.

From the perspective of the educational setting, the digital age has created new concerns regarding the use of non-traditional electronic and Internet resources. The speed with which students acquire information technology skills may be chronically outpacing educators' abilities to ensure that positive habits of on-line behavior are being formed. Therefore, *Cyberethics, Cybersafety, and Cybersecurity* issues need to be integrated in the educational process beginning at an early age. Unfortunately, while the teaching of technology processes and skills has been handed to the classroom teacher, most educators lack the knowledge and up-to date information related to Cyberawareness issues, particularly with respect to security. Teacher technology training has been geared toward skills development and integration techniques. Teachers, in many instances, model incorrect protocols and behaviors to their students. Not only does this increase the risks to the security of the teacher's own classroom and local school system's information systems, but it also increases the chances that students will mimic these behaviors. This can have negative impacts on systems at either home or work.

When I first came on board at the University of Maryland, the National Teacher Technology Standards (or NETS-T) were just starting to surface—you should have a copy in your handouts. While there are certainly a number of standards to address—ethical and safety being one (standard 6) the primary focus was and continues to be on getting teachers to utilize the technology—initially this has focused on computerizing administrative and productivity tasks. It has been an exciting time as much progress has been made, but at the same time, we still have a long way yet to go. NCLB has focused attention on accountability and meeting AYP—and technology efforts have been to help teachers understand technology to provide them with a means to analyze and interpret data – a central tenet of NCLB. There has been a growing focus on using technology for differentiating instruction to help all students meet benchmarks. As you can see while there is a steady push for educators (admin/media teachers) to utilize technology, clearly there needs to be a push for cyberawareness—safety, ethics and security, as we need to protect the important data that we are collecting, analyzing, and interpreting.

My role at the University of Maryland, as Director of Educational Policy, Research and Outreach, calls for significant interaction with teachers in the classroom, both to give professional development, but also as an observer. When visiting teachers (both pre-service and in-service) it's exciting to see them using technology—both to support their teaching and as a means to engage their students, however it is quite eye opening to see the poor cyberpractices that occur without anyone even noticing. For example:

- **PowerPoint presentations using materials, graphics, pictures without citations/proper references**
- **Student projects where students have downloaded music files to play in the background and teachers are "impressed"**
- **When showing students' Internet sites, a *popup* will appear, and the teachers click OK to continue without even reading what they are doing. Untold amounts of spyware can be on their computer.**
- **Having students come in with floppy disks and using them on the school's computers without proper virus scanning. When I bring home work from the teachers, the virus software on my computer gets quite a work out.**
- **Teachers explain that they opened up a virus attachment because they wanted to see what it "looked like" or what "it did."**
- **Leaving passwords on sticky notes next to computer. (How many grade changing scandals have we heard about? – too many.)**
- **Going to generic websites that list possible "pen pals" to start global class projects, without trying to emphasize the importance of verifying that the e sites are legitimate. This can result in students dialoging with potentially nefarious users.**

I could go on, but these are just a few items that highlight the need for teachers to understand the importance of Cyberawareness in today's setting—not just using technology but using and modeling correct behavior.

Within the College of Education at the University of Maryland, we recognized the need when NETS*T rolled out, and we have developed a number of initiatives to help provide some of this material to the community

- **A free self paced tutorial for students on the basics of C3**
- **Both a 1 credit and 3 credit course on C3 for pre-service and in-service teachers**
- **A C3 portal for faculty, students and teachers to find resources related to C3 for the classes and research**
- **Preparing for our 5th annual C3 conference – which has a stronger focus on cybersecurity issues**
- **K-12 lead partner in a recently awarded NSF ATE (**Advanced Technological Education) Center-CyberWATCH. This includes a continuation of the efforts already described (conference, portal), but we are also developing materials and initiatives for teachers and conducting research to explore the needs, gaps, and possible solutions in this area
- **C3 blog**

- **National surveys to gain insight into the nationwide problem and gather anecdotes of best (and worst) practices**
- **Monthly professional development on TappedIn.org (C3 Monday)**
- **Interactive calendar—for the months of April (C3 awareness) and October (cybersecurity)**

Even with all this we have only begun to scratch the surface when it comes to what is needed. I am excited to see others like the NCSA recognize the importance of this topic –because it will truly take everyone working together to help raise awareness of this issue. To truly impact the educational setting, both formal and informal initiatives need to be present. The creation of more and more programs, such as the C3 Conference, the CyberWatch Center, C3 courses and professional development, blogs, surveys, etc., promise to help address this knowledge gap. I look forward to working with the National CyberSecurity Alliance, and all of you here, as we work to have our cyberawareness catch up to with other technology training.

Thank you.