

Information Technology

<http://chronicle.com/weekly/v53/i18/18b02901.htm>

From the issue dated January 5, 2007

We Must Educate Young People About Cybercrime Before They Start College

By SAMUEL C. MCQUADE III

With the start of this new year, the United States formally becomes a party to the Council of Europe Convention on Cybercrime, marking another major development in worldwide efforts to combat high-tech crime. However, the convention, despite being the first international treaty on cybercrime, is more of the same: Fifty years after the onset of documented computer abuse in the United States, our efforts to curb it have helped very little. We continue to seek technological, legislative, and law-enforcement solutions to what is largely an educational problem.

Parents and teachers are increasingly relying on new technology to enhance education both in and out of the classroom. Employers are badly in need of competent and ethically responsible computer users. Meanwhile, our schools have failed to systematically incorporate Internet safety, information security, and cyberethics instruction into curricula.

Society cannot afford for this to continue — and higher education should help make sure it does not.

A growing body of empirical research strongly suggests that adolescents and young adults are increasingly becoming both victims and perpetrators of crime and abuse enabled by information technology. The long list of offenses is familiar to those of us on college campuses: academic dishonesty; intellectual-property theft; piracy of music, movies, and software; online threats and harassment; credit-card fraud; unwanted solicitations for sex; and writing and distribution of malicious computer code.

Consider the findings of several recent studies:

- Seventeen percent of students surveyed in 2004 by my institution, the Rochester Institute of Technology, reported that they had been harassed online. Eight percent said they had been threatened; 6 percent had been cyberstalked; and another 6 percent had been victims of identity theft. One in three claimed to know the perpetrator prior to the crime. That shouldn't be surprising, given that the students also admitted to being offenders — especially in instances of pirating and academic dishonesty.
- One in three children ages 6 to 17 reported having been victimized online in a 2005 study on cyberbullying conducted by University of Wisconsin and Florida State University researchers. The respondents also reported feeling angry, sad, or depressed as a result, and often did not tell their parents about the incidents for fear of losing computer privileges.
- A 2006 national study of online youth victimization conducted by University of New Hampshire researchers found that one in seven reported receiving unwanted sexual solicitations. One in three received unwanted sexual material, and one in 11 experienced harassment, including threats.

Young people of all ages and from all socioeconomic backgrounds routinely use small, affordable, and interoperable gadgets such as minicomputers, cellular phones, PDA's, digital cameras, and MP3 players in

their schoolwork and social interactions. They are often allowed and encouraged by parents to use such devices to browse and download Internet content, send text messages to each other, play electronic games, shop online, and post personal information (true or false) to any number of popular social-networking Web sites.

Unfortunately, they often do so with little regard to the permanency of content posted on the Internet, or potential consequences of sharing intimate details or photographs with the world. Following years of computing, often with inadequate supervision, many arrive on college and university campuses both technologically savvy and naïve to the dangers that same technology poses.

Last May the Web site Bad Jocks published photos of the Northwestern University women's soccer team in an alleged hazing incident. Various photographs included players shown in their underwear, handcuffed, or with their hands tied behind their backs. Two days later, Bad Jocks posted photos of similar activities by athletes at 11 other colleges. Those episodes inspired fresh discussions about acceptable computer use during many orientation sessions.

Why are we waiting for kids to arrive on our campuses before we intervene? After all, these are the next generation of employees, the same men and women who will be using — and perhaps abusing — an already vulnerable information infrastructure that is critical to the functioning of our society.

To its credit, the federal government has stressed technological, legislative, and law-enforcement solutions to these problems. Efforts to protect children have frequently focused on the dangers of adult sexual predators and efforts to prevent minors from gaining access to pornography.

In the last decade, the federal government has also established a variety of panels to help prevent Internet crimes against children. Internet safety guides and educational Web sites have been created. Two national youth Internet-safety surveys and online instructional tools have been established: NetSmartz, developed by the National Center for Missing and Exploited Children, and i-SAFE, developed by the nonprofit organization for which it is named. And last year the Department of Homeland Security announced a national education round table intended to raise public awareness about the need for K-12 Internet safety, information security, and cyberethics instruction.

Those and similar efforts are notable, undoubtedly helpful, and terribly inadequate. Even collectively, they do not deal with the fundamental challenge we face: how to systematically deliver needed instruction to the nation's elementary and secondary schools, which are managed by a myriad of state and local governments. No school system is known to have systematically provided training for teachers, nor implemented cybersafety, cybersecurity, and cyberethics instruction in all grade levels.

In July, however, Virginia enacted legislation directing that state's Department of Education to issue guidelines to school districts now required to provide Internet-safety instruction. That may help remedy the problem of ad hoc instruction by conscientious teachers, who select from a potpourri of available (and often unevaluated) online teaching aids in order to squeeze some information into a block of instruction. I suspect few of them are ever acknowledged, much less rewarded, for doing so.

Virginia will be challenged to deliver on the intent of its new law since school districts already strain to provide adequate instruction in "the basics" — not to mention meet the demands of legislation such as the No Child Left Behind Act. Educators rightfully worry about another topic being heaped onto their pile of things to teach, especially when many of them are themselves unfamiliar with computer technology and the danger it poses. And regardless of what schools may do to block Internet access to unacceptable content, Wi-Fi transmissions emitted from nearby buildings, along with cellular satellite connections, mean that principals have effectively lost control of digital communications on their campuses. What kids cannot do with their school computer under the watchful eyes of a teacher, they can readily accomplish on the playground or on a

school bus with their portable electronic devices.

There is little, if anything, we can do to prohibit access to these devices, although a few school districts are beginning to ban use of them by students on school property. By and large, they have become ingrained in our society and our schools. Yet we have ignored the need to teach students how to use the devices in a manner that is safe, secure, and ethical.

Here are six steps higher education should take to help foster the educational and work-force training reform that is needed in this country:

1. The academy needs to conduct far more research to verify the nature and extent of cyberoffense and victimization by and among adolescents. Criminologists already recognize the longstanding dearth of empirical studies on computer crime. The number and quality of theory-driven studies that examine such crimes, as well as general computing practices and information-security abilities, are nearly nonexistent.

2. In partnership with local schools, we should greatly expand the evaluation of instructional materials and efforts to use them. We should also evaluate student learning and knowledge retention over extended periods of time.

3. Colleges should create models of the best computer-use policies and serve as technical advisers to local school systems, which often have limited IT expertise. That would provide an opportunity for faculty and staff members to work together to aid community-education efforts.

4. We should also lead by example in revising curricula to ensure that computer literacy among college graduates includes the skills needed to protect information systems and to use all forms of IT responsibly. This is especially important at institutions that specialize in teaching future teachers. Perhaps IT professors could team-teach particular courses to jump-start this process, with a goal of helping teachers in training to integrate basic cybersafety and security concepts into their instruction. Where is it documented, after all, that cybersafety and cyberethics cannot be covered in English, history, health, or mathematics courses?

5. Many colleges and universities are well positioned to add Internet safety, information security, and cyberethics training to continuing-education courses as well as to degree-program requirements. Higher-education institutions could also offer leadership training to executives of public, private, and nonprofit organizations who have vested interests in having employees who can secure, maintain, and responsibly use information systems. Such training would demonstrate higher education's concern for community and national well-being through promotion of responsible computing — and could serve as another source of revenue for institutions.

6. Higher education should offer training for little or no cost to public- and private-school officials, teachers, and parents, as well as to adolescents, possibly even through joint instructional sessions. After all, societal problems of this magnitude call for integrated solutions, and young and older people depend upon and share computer devices, data, and networks. If campuses can play host to events for high-school and even younger students, why can't we organize some of our community outreach (and recruiting) efforts around this vital issue?

Those and other strategies need to be carefully considered and supported in ways deemed appropriate to schools and communities. In Rochester more than 20 school districts are actively exploring these issues with RIT, with help from the National Center for Missing and Exploited Children, the Information Systems Security Association, and the FBI's InfraGard — all leading organizations that share RIT's vision for initiating and modeling what should become a national reform movement.

Higher education can and must help to prepare graduates who can keep America's computing society safe and

secure. We must reach out to our schools and to employers to assist them in putting instructional programs in place. We cannot wait for them to magically figure this out for themselves.

Samuel C. McQuade III is graduate-program coordinator at the Rochester Institute of Technology's Center for Multidisciplinary Studies and author of Understanding and Managing Cybercrime (Allyn & Bacon, 2006).

<http://chronicle.com>

Section: Information Technology

Volume 53, Issue 14, Page B29

[Copyright](#) © 2006 by [The Chronicle of Higher Education](#)

[Subscribe](#) | [About The Chronicle](#) | [Contact us](#) | [Terms of use](#) | [Privacy policy](#) | [Help](#)