The Not-So-Distant Average School Day

Mary O’Dea
Wayne Rich

Sixteen year-old Harris is beginning his school day in Buffalo, New York. He’s scheduled to meet with his art group this morning at 10:00 AM. His group consists of five students who are roughly the same age as Harris. They are lead by their instructor, Ms. Rodriguez, who is just finishing her early morning cup of coffee in Santa Fe. Harris enjoys the work he does for the course, and he’s looking forward to sharing his latest interactive video project with his group.

As Harris finishes his breakfast, he takes a seat at his laptop – the one his school provided – and boots it up. This morning he’ll meet his group in the classes’ assigned chat room, at the scheduled time. His teacher, of course, will be there, as will his classmates, even though they live scattered hundreds of miles apart. This school has no traditional walls other than those used for administrative purposes, yet it graduates hundreds of students each year and offers classes to other students who must fulfill their own schools’ graduation requirements. It is, of course, a completely paperless environment. All of the schools’ courses are taught this way, and the school is typical of the times.

As Harris logs on to his laptop, he must complete a series of steps to get onto the Internet and then into his classes’ chat room. Earlier this year, when he opened the new computer from his high school, he had to complete an Internet Safety course – which included getting a parent’s signature – before he could log on to the Internet. He was issued a certificate upon completion and the information from that completion had to be sent to his school before he was allowed to participate in classes. He will have to do this each time he begins a new class, or set of classes, with the school. If he wants to use a computer other than his own, it will be necessary that he use his certification information to use the Internet.

Several hours pass, and Harris finishes his time with his classmates. He’ll head downtown now for his business class. He’s interning at a local shop, earning credit for school while he’s learning basic accounting and business skills. He’ll log his intern hours every day with the school, via the Internet, and weekly his supervisor will communicate with his instructor in Birmingham to make sure Harris is gaining the necessary skills. Every two weeks, Harris will take an online test as part of his class requirements. Once again, before logging onto his school account, he’ll need to supply the necessary certificate information before he will be allowed to go online.

Harris’ week continues in the same vein. He won’t set foot in the type of classroom our generation is accustomed to. At times, his classes may meet at odd hours in order to accommodate schedules and classes offered around the world. Internet and varied communications technologies will be necessary for any child to complete a school education. Harris’ elementary-aged sister spends several hours a day at the “school” provided by her mother’s business as her mother works.

Basically, this is a gathering of elementary-aged children, too young to be unsupervised, who will accomplish work at the facility just as Harris did at home. These children, too, will have taken an age-appropriate Internet safety certification course prior to getting online to do school work. Much of the youngsters' work will be completed from home, as their parents and older siblings will spend much of their time working from home as well.

While this scenario is certainly only one of many possibilities, it provides modest insight into the realization that technology will play an ever-increasing role in our children's lives as in their educations. As we continue to increase the use of technology in our lives, and our children's lives, we must increase our awareness and preparation for the increasing threats posed to our children by criminals familiar with the cyber world.

> *"The more that we use the Internet, the more likely we are to forget to do the things necessary to keep our data, ourselves, and our family safe online. It is this* complacency *that we must struggle with every time we sign online." (www.Secureflorida.com).*

A Double Edged Sword: Technology and School Children

There is little doubt that in the near and far-term future, technology will be increasingly available to children of all ages. Clearly the availability of technology to our youngsters is a boon to learning, education, and open communications. For obvious reasons, though, it creates the possibility of an ever increasing threat to the personal security of anyone naïve to the methods of cyber criminals. It stands to reason that as the use and availability of technology increases, a logical way to begin to ensure awareness is through our schools. It's an old, but true, premise that the best place to begin social awareness is with our children. As we teach our children – and their parents – about safety on the internet, for example, we begin a cycle of awareness that perpetuates through the ages.

In both traditional and non-traditional constructs of schools, technology will increasingly be used as an educational tool in the foreseeable future. In one example, in a first of its kind program, the state of Maine has partnered with Apple Computers in order to supply all of the states' seventh and eight grade public school students with laptops. Virginia is following suit with negotiations for computers from Apple and Dell, and Philadelphia partnered with Microsoft to open its School of the Future: a no-paper, no-textbook, high-tech high school. Maine's program, now in its second year, is working well, and is a success for the state and the students. The laptops are wonderful educational devices, but experience also tells us that putting laptops into the hands of school-aged children, or anyone unaware of personal security safety problems, can be a dangerous prospect.

The answer, of course, is not to stem the flow of technology to our children but to work to protect them. It's imperative that we arm our children

– and their parents – with the ability to protect themselves against cyber crime. With laptops and PC's in the hands of, or at least available to, nearly every child in the U.S. right now, internet security is an ever increasing issue that schools, counties, and governments will become progressively more involved with.

Awareness is the most important aspect of ensuring safety for our children and their children. Society is in a state of technological transition. As adults and parents, how many of us recall pre-computer and pre-ATM days? While many of us utilize computers on a daily basis, how many of us are fully aware of the techniques needed to protect ourselves, let alone our children? We may be continuously bombarded with virus warnings on our computers, and we may witness cyber stalkers being arrested on our televisions, but are we actively doing enough to protect our youngsters and to teach them how to protect their own children when the time comes? How many of us don't keep up – or are even aware of – parental blocks we can use to protect our kids? How often do our children go unsupervised in front of a computer screen?

As in many other educational domains, the most evident place to begin helping our children to protect themselves against cyber crime is in the schools. It also follows that because cyber crime is a criminal act, some of our strongest lines of defenses against it are our police departments and law enforcement agencies.

Right now, school districts and counties across the country are encouraging students and parents to practice cyber safety. They're offering classes and websites to help people learn how to take care of themselves and children in the cyber realm. This is the first step in protecting and teaching our children and ourselves. The FBI and the Office of Juvenile Justice and Delinquency Prevention (through the Internet Crimes Against ChildrenTask Force) both offer very insightful and informative information via their websites regarding internet crimes against children, how to prevent them, statistics regarding the crimes, and state and local offices.

While no one can deny these, and many more across the country, are powerful weapons against cyber crime, encouraging education may not be enough. After all, many parents who are concerned for their children's safety are already aware of how to protect their children, or they are likely to find out by voluntarily attending school or local seminars regarding the subject. It is those children and their parents who are unaware of the need to take precautions or how to take those precautions who are most vulnerable. These are the people who we most need to target. Perhaps, then, it is a wise choice to mandate cyber safety education whenever possible.

Maine Is Doing It

In Maine's prototype program, during the first years, the state brought laptops into public middle school classrooms (2002-2006). Schools were encouraged to implement Internet safety programs, but they were not required to do so. The lack of a mandate was more a reflection of the political climate at the start of the project than of a value statement about Internet safety.

Last year, the Attorney General's Office and the Department of Education teamed up with NetSmartz.org, a well-known Internet safety group. Since then, “as part of the participation agreement, [the state] mandated that schools implement an Internet Safety program, [and they] continue to work with the AG’s office and with NetSmartz” says Jeff Mao of the Maine Department of Education.

If Maine serves as precedent, we should be working to mandate Internet safety programs in our schools. This is easy enough to do, as Maine did, as part of a participation program, and parents can be brought into this fold. If not as a requirement for participation, then local, state and/or federal authorities can mandate this education as curriculum required to maintain accreditation or funding. Requiring students and parents to complete at least a basic awareness program (which could be done online, at local libraries, etc) will assure that we educate more students than on a voluntary basis. Additionally, this requirement need not be tied to only those schools supplying students with their own computers. Since schools are sometimes the main source of computer exposure for some students, it is a natural place to require safety training prior to allowing computer use.

The Role of Police Departments

Since 1983, the D.A.R.E. (Drug Abuse Resistance Education) program has worked to give “kids the skills they need to avoid involvement in drugs, gangs, and violence.” (www.dare.com). Why not use this program as a model for educating children about Internet safety? Training police officers to help children become aware of and avoid Internet safety problems seems an obvious place to begin, and it promotes interaction between police and children at the same time it helps prevent terrible kinds of crimes. The D.A.R.E. program is widely accepted as having very positive results with school children. As a well established program, we suggest either adding cyber crime to the D.A.R.E. program curricula or building a similar program for cyber crime. Another advantage of “merging” with the D.A.R.E. program is the long list of supporters and sponsors that help to finance the ongoing project, making cyber crime education more affordable, thus more readily available, to a variety of clients. Ideally, programs such as D.A.R.E. will be coupled with consistent, recurrent programs within schools to ensure that students of all ages, abilities, and backgrounds are provided the tools necessary to protect themselves against a variety of cyber criminals.

Although there is no way to guarantee the prevention of cyber crime, there is much hope in raising awareness. As today’s children mature, our society will become more attentive to the hazards of cyber crime as well as the skills needed to help prevent it. Today, our job must be to immediately educate people of all ages about potential dangers to cyber space users. We must remember that technology changes “faster than the speed of light,” and the future may hold even more pitfalls for the next generations in the cyber world. Still, with any luck, education today will sustain our children through adulthood, and they will have the ability to protect the children of the future.

Related Websites

http://bob.nap.edu/html/youth_internet/
www.dare.com
http://www.fbi.gov/publications/pguide/pguidee.htm
http://www.globalgateway.org.uk/Default.aspx?page=390
http://www.hackerhighschool.org/
http://www.icactraining.org/default.htm
http://www.lhric.org/security/desk/letter7.html
http://www.isecom.org/
http://www.netsmartz.org
http://www.npr.org/templates/story/story.php?storyId=6210622
http://www.secureflorida.org/
http://www.state.me.us/mlte/
http://www.whitehouse.gov/news/releases/2002/10/20021023.html
http://www.whitehouse.gov/news/releases/2002/12/20021204-1.html
http://www.whsv.com/news/headlines/4308577.html