A few months ago, I invited Scott Charney to expand on his ideas about educating children about ethical use of computers and networks in the age of the Internet. Charney was chief of the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division at the U.S. Department of Justice (DoJ) from 1991 to 1999. He worked as a principal for PricewaterhouseCoopers and then in January 2002, Microsoft announced that he had agreed to become the Chief Security Strategist for the corporation. Mr Charney has written the following essay on how adults can help ensure young people learn the basic rules of PC security and privacy; education programs can direct talent into positive pursuits. The following is the text he has very kindly sent me for publication in this newsletter.

* * *

Teaching the Golden Rule in the Computer Age
By Scott Charney

With each new report of a young person caught hacking into a computer system or circulating a computer virus, we get another stark reminder that for some kids today, traditional notions of ethics and piracy are missing, at least when they log onto their PC. But it’s not entirely their fault. If you compare just how differently computer technology enters our kids’ lives, as compared to the way previous generations learned about powerful technologies, you realize that kids need our guidance to learn and apply old rules to new technology.

Think about other powerful tools, such as automobiles. Automobiles are given to adults first, and then those adults, whether parents or teachers, educate younger individuals on the appropriate use of the technology. Computers, of course, are introduced in exactly the opposite way; children are given access to a powerful technology that, too frequently, neither their parents nor teachers fully understand.

In the days before script kiddies (unsophisticated hackers who run powerful hacking tools), a victim such as the United States Government could often tell whether a hacker was a serious threat. A hacker who was hunting and pecking on the keyboard, or having difficulty with programming syntax, was clearly unsophisticated. In such cases, it was sometimes appropriate to deal with the hacker by discussing his behavior with his parents. The scenario was often the same. Federal agents would explain to shocked parents that their son (it was almost always a boy) was hacking into the United States Department of Defense; the parents would respond with the same three statements: (1) it was great that their son had a hobby; (2) it was a high-tech hobby which might be of future value; and (3) at least their son was safely in his room and not out roaming the streets. These answers were all true but missed the basic point: adults needed to take responsibility and manage their child’s use of this powerful technology.
What brought the problem into sharper relief were presentations to youngsters about computer ethics and respect for privacy. When asked if they would read their friends diary or enter a neighbor’s home if a window was open, the answer was “no.” But when asked if they would hack another person’s machine, the answer was often “yes.” The reason, of course, that children do not read a friend’s diary or enter a neighbor’s home has everything to do with education. Children are taught, at a young age, to respect the physical property rights of others. Unfortunately, adults did not react to the explosion in information technology with a massive campaign on ethical computing.

In sum, there has been no one to pass along society’s collective rights and wrongs for PC use and Internet browsing. So kids do what kids often do when there’s little adult guidance; they look to each other or develop their own rules, sometimes with costly and potentially dire consequences. For example, a young hacker in Massachusetts disabled an electronic telephone switch, preventing airlines from remotely switching on landing lights at a regional airport and forcing planes to be rerouted to other airports. Computer viruses spread by hackers including some quite young, have collectively caused billions of dollars of damage to governments, business and home PC users.

Even more troubling are the implications of seemingly innocent hacking in a post Sept. 11 world. Security experts must waste precious time and resources investigating all electronic intrusions, and could miss a potentially catastrophic attack while investigating a hacker with little or no evil intent.

The future of some of our most talented youth is also at risk. Once the unchanneled talents of young computer whizzes lead them to the wrong side of the law, there’s a strong possibility that they will get stuck there and eventually tarnish their future with a criminal record.

As educators and parents, there are things we can do. We can learn more about what our kids are doing during those endless hours they spend online. We can take the time to learn about the risks, set appropriate rules, and regularly talk to our kids about these guidelines, ones that mirror the standards we set for our kids in other parts of their lives. Simply put, if it’s not OK for Johnny to snoop in his sister’s hardbound diary, it shouldn’t be OK for him to crack the password of a private e-mail account and read another family member’s mail.

That said, we shouldn’t stifle young people whose talent and perseverance allows them to master and manipulate sophisticated technology. We should harness this talent to benefit these young people and society. Let’s consider offering more lawful contests that challenge young people to test the security of computer systems. We might also create programs that help young people further develop their interest in technology into successful, lifelong careers.

If we are successful, things will hopefully be different when today’s young people hand over the keys to the family computer to their kids.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.
