My Turn: There's One More Talk You Need to Have

You've tackled sex, drugs and alcohol. Now you need to find out what your child is doing online

Martha Stansell-Gamm, head of the Justice Department's Computer Crime and Intellectual Property Section, says parents should pay more attention to what their kids are doing online.

By Martha Stansell-Gamm
NEWSWEEK

Sept. 15, 2003 - Not long ago my son received his driver's license. In Virginia, this is a big deal-the ceremony takes place at the county court where a black-robed judge, a police officer and a defense attorney all address the drivers about their newly acquired freedom. It is an impressive rite of passage that marks a teenager's assumption of important new powers and responsibilities.

As I watched the ceremony, I was struck by the difference between our approach to teaching kids to drive and teaching them to use computers. Cars and computers are both powerful tools that can do wonderful or terrible things-depending on whose hands are on the wheel or whose fingers are on the keyboard. Most parents know that inducting a teenager into the world of driving requires more than teaching him the mechanics. (Imagine it: "There's the gas pedal, steering wheel, brake and keys-have fun, dear!") They tell their kids that irresponsible behaviors like driving drunk and speeding endanger others on the road. But because most parents did not grow up using computer technology (and may even fear it), they don't understand how much damage kids can cause with computers. Our children, however, know this well.

Years ago, when my son was in elementary school, I spoke at a career day where I posed the following question to his fellow fourth graders: "How would you feel if you wrote an e-mail message to a friend and someone hacked your Internet service provider and read it?" They were horrified! I went on. "How about if someone hacked the school computer and read your grades?" The group was unanimous and passionate: anyone who would do such a hurtful thing was the scum of the earth.

Afterward the teacher approached me privately and asked, "Can children actually do those things?" Yes, they can, and it's not that difficult. Any moderately bright teenager can do all that and more, aided by free point-and-click hacker programs openly available on the Net.

Unfortunately, many parents don't find out what their children are doing online until the FBI appears at their door with a search warrant. A teenager can (and did) cut off the phone service to an entire town for hours by hacking the local phone company. Adolescents can (and have) seriously hurt the music, gaming and software industries, shut down Internet news and commerce sites, brought businesses and government agencies to a halt, and attacked military networks in ways that have initiated high-level concern for the economy and for public health and safety.

How can we teach our children to use computers responsibly, just as we teach them to be good citizens of the road? Talking to them is a great way to begin. Although it may sometimes seem that it doesn't matter what we say to our kids, most of them are listening. Adolescents who are charged with online crimes-like the 18-year-old arrested for creating a variation of the Blaster virus that instructed at least 7,000 computers to attack Microsoft networks-almost never have criminal records. This is most likely because they absorbed the values their parents taught them about other areas of their lives. Many kids who would never steal mail or CDs or destroy property think nothing of helping themselves to copyrighted music over peer-to-peer networks, or launching a destructive Internet virus.

Parents don't have to be technologically savvy to tell kids what's off-limits. They need only to make it clear their children must respect the rights of others. They need to tell them that no matter how many of their friends are stealing music, movies, games or software, they are not allowed to do it. (In fact, parents should make sure kids remove file-sharing programs from their computer. It's a security hazard, too.) They must be explicit that hacking or attacking networks is wrong. And they need to make it clear that if these rules are broken, the child will face serious consequences-at home, at school and maybe even in the courts.

There are resources to help parents teach their children how to be good citizens on the Net. A good place to start is www.cybercrime.gov; university-sponsored ethics Web sites are also excellent sources of information. But the most important thing parents should remember is that they don't have to be information-technology experts to have these core ethics conversations, and there is no voice a child needs to hear on this subject more than theirs.

Stansell-Gamm is the chief of the Computer Crime and Intellectual Property Section at the Department of Justice.

© 2003 Newsweek, Inc.
Posted on www.cybercrime.gov with permission of Newsweek, Inc.