Hackers: What Role Does Education Play?

Joseph J. Jaksa, Anne R. Tapp
Saginaw Valley State University, University Center, USA

With the instant availability of information on the Internet and lack of exposure to digital citizenship, students’ temptation to become a hacker and potentially execute destructive acts using technology is real. The message of digital citizenship needs to start early in the education process and be reinforced at every level. It is essential to embed these lessons of ethics within curriculum. Teachers need to be leaders of digital citizenship in their respective schools and communities.

Keywords: character education, digital citizenship, cybercrime, ethics, liability

Introduction

Teenage hackers are not news today. Junior high school-aged students have demonstrated their ability to create a virus or worm, perform illegal downloads, and gain illegal access to documents or systems. Ethics in computing needs to be addressed at an early age, well before middle school. Historically, children learned from adults through direct observation, apprenticeships, and schooling, and adult behavior was modeled through various interactions. As technology progressed, the adults on television, films, and other media began to play a larger role. Yet, teachers, parents, neighbors, coaches, religious mentors, and other face-to-face, real-time interactions still exerted a viable influence on children. Today, children can now learn directly from experts and become experts themselves via the Internet or with software without face-to-face mentoring or interaction. In many cases, adults feel that children know more about how to manipulate the technology.

The Internet is a powerful environment for enhancing the transfer of social and emotional skill development. It is replete with teachable moments when young people are challenged to exhibit self-control, engage in critical decision-making, and express feelings while demonstrating respect and tolerance for others. Many districts have a 1:1 technology use plan and are encouraging students to bring their own electronic devices to class. As schools have increased the amount of access students have to cyberspace, the application of social skill training to this setting has become increasingly apparent (Berson, 2000, p. 159).

Today’s Internet or World Wide Web was designed to be a medium for communication and interaction. The unfortunately reality is that today’s Internet was not designed nor intended to be protected. Because of this harsh actuality,deviance and crime run rampant. The term “hacker” is often misused or misrepresents the actions by the individual. Typically, “hackers” are individuals who gain unauthorized access into computer networks as a sort of an “electronic joy-ride.” The actions of a hacker are simply to investigate or look around the end user’s system or site. Conversely, an individual who gains unauthorized access into a computer network or system, with the intent to cause damage or harm, is actually “cracking” into the system. Society as a whole
refers to all individuals gaining unauthorized access into a computer network or system as a “hacker,” regardless of malicious intent. These individuals can be curious school children seeing the amount of access they may be able to gain within a computer or network system as well as more seasoned cyber criminals seeking destruction, profit, or both.

Hackers are commonly classified into four different categories according to their ability and desire. “Script kiddies” are novices when it comes to hacking. They have very little experience intruding into electronic systems and developing programs to carry out these tasks. The script kiddie may use a hacking program that has previously been developed to gain unauthorized access into computer systems. Advanced and well organized hackers can be classified as “white-hat,” “black-hat,” and “grey-hat” hackers. White-hat hackers actually work for the betterment of the computing system or a specific organization. They attempt to gain unauthorized access into systems to help organizations address and remedy these problems or issues, so others cannot infiltrate the system. Black-hat hackers enter into computer or operating systems without authorization and for the purpose to cause damage or harm. Black-hat hackers are frequently involved in various types or cybercrimes or electronic devious acts. Finally, grey-hat hackers look for opportunities to gain unauthorized access into computer or operating systems, and then commonly notify the organization of their actions or success while informing the organization that they can correct the flaw or show how to correct the vulnerability for some type of fee (Code and Command, 2015). The evolution of a hacker can be a fairly fast process when young students are introduced to computer technology and quickly adapting and integrating into workings of these systems.

Implications

Education plays a critical role in the solution of this problem, as it affects all-aged students and helps shape the future of society. Schools must lead the effort to ensure that young people learn to use the Internet in a safe and responsible manner, as they are the most universal location where United States (U.S.) students are learning how to use the Internet. Schools are a well-placed, efficient vehicle to provide education to and partner with parents, libraries, and other community organizations to create a community-wide effort.

Even today’s rapidly evolving cyber community. Laws have been established to address the threat of hacking. For example, all fifty states in the U.S. have created laws addressing unauthorized access into computer systems (National Conference of State Legislatures, n.d.). In addition, the U.S. Federal Government has also developed laws pertaining to hacking and other unwanted or illegal intrusions (Hacker Law, n.d.). With these laws defined, schools and their districts must understand what type of actions define hacking on the state and possibly the federal levels.

In the event, students utilize school equipment and computer infrastructure to commit hacking crimes, the school district could be held liable for the crime or infraction on either a criminal or civil level. Any damage created or caused by a student using school property and infrastructure could result in charges against the specific school district.

It becomes imperative that all school districts teaching computer technology or allowing students (and employees) to access the World Wide Web on school property to develop policies and procedures addressing appropriate conduct and actions. Policies should address acceptable and unacceptable practices, while using school or school district equipment of infrastructure and have the policies and guidelines carefully reviewed and vetted by a qualified legal representative. These policies and procedures should include student use and
WHAT ROLE DOES EDUCATION PLAY

conduct as well as contingency response plans by the school district in the event of an unwanted action by students or by employees. School districts and the educational staff must remember that ignorance is not a defense in our court systems and criminal and civil charges can be brought against a school district for damage caused or created using school-owned equipment and infrastructure.

Character education programs seek to impart good values to young people. One potential problem with many of these programs is that they are frequently rule and punishment-based. On the Internet, inappropriate behavior frequently goes undetected and thus unpunished. When working with young people using the Internet, it is important to keep in mind how features of the technology can impact ethical decision-making. As young people grow, their ethical decision-making is largely influenced by external factors. The two most significant external forces are perception of the harm they have caused by their actions, which leads to feelings of guilt and remorse, and fear of detection, which could lead to punishment or loss of reputation according to Kohlberg’s theory of moral development (Crain, 1985). Technology interferes with both of these external forces. When we use technology, we are distanced from recognizing any harm that we may cause. We also feel invisible. As young people are growing up using the Internet, we must enhance their recognition of potential harm caused by their actions and diminish their perceptions that they are invisible. Our character education programs must focus their attention on enhancing internalized control through an understanding of how our actions can cause harm to unseen others.

Students who are determined to be at-risk for other behavioral problems, especially school “outcasts,” are also the ones who are most at-risk of becoming involved in negative activities on the Internet. Educators must recognize that any student who does not feel a part of the school community is likely to be finding an online community or an individual predator ready and willing to exploit his or her loneliness. Helping students feel connected and cared for in their home, school, and community takes on even greater importance in recognition of the potential that young people who do not feel connected and cared for are extremely vulnerable on the Internet. Ethical, safe, and socially conscious online behavior may positively transform the nature of social interactions among youth and counter the betrayal, coercion, and deception that accompany destructive behavior.

Children develop very powerful theories of the world by the time they are four years of age. A single experience with ethics in high school will not be able to wipe out years of beliefs and behaviors (Gardner, 2004). Even if students maintain the message from age five onward, in adolescence, they are prone to changing their minds. If schools continue the ethics message from an early age throughout the teenage years, they might have a chance to maintain the belief system.

A task that is beyond the skill of the individual will cause anxiety. A task which is below the skill of the individual will cause boredom. The task that provides challenge, discovery, and resolving problems gives enjoyment to programmers (Himanen, 2001). The main motivation for hackers was how creative they felt when working on a project.

The hacker identity includes solving coding problems, having fun, and sharing code at the same time (Lakhani & Wolf, 2005, p. 6). Ankit Fadia, a 16-year old hacker said, “Hacking really gives you the power to do things that normally people do not know about. It gives you the power to make a computer work the way you want it to work. So, the adrenaline rush associated with hacking.... Initially, it is the forbidden that attracts—Hacking is usually something that is forbidden. So that originally got me interested. And then the knowledge part came in. So, the power of knowledge is really what got me interested in hacking” (Moyes, 2001).
An analogy can be made between driving a car and using computer technology. With driving, children from an early age observe adults completing this task. They observe both good and bad examples, hear the standards, learn to distinguish between what is right and wrong, and receive formal training. With computer usage, it is different. Most parents do not possess Internet usages skills to the degree of their children, so how can they exhibit best practices to them? Most teachers cannot write a piece of code on the computer, so how can they exhibit best practices and ethical behavior to future hackers?

Educational institutions need to model ethical practices with technology. Presently, there are standards, such as International Society for Technology in Education’s (ISTE) National Educational Technology Standards for Students (ISTE, 2000) as well as other initiatives, such as the Ten Commandments of Computer Ethics (Computer Ethics Institute, 1992), and Digital Citizenship. Nationally, there have been concerns by the U.S. Department of Justice and the Federal Bureau of Investigation (FBI) for schools to teach digital citizenship/cyber ethics. The concept of Digital Citizenship was designed to help leaders of technology understand what students should know, how students should appropriately use technology, and how to best prepare students. Digital citizenship teaches appropriate, responsible behaviors for when using technology as well as issues in online safety. There are nine elements to this curriculum introduced in kindergarten and reinforced throughout students’ educational careers: digital access, digital commerce, digital communication, digital literacy, digital etiquette, digital law, digital rights and responsibilities, digital health and wellness, and digital security.

The safety and well-being of children is of utmost importance to educators. However, the reality is that few professionals are prepared for this role in terms of technology. As children and youth increase the time they spend online, they also are progressively immersed in an environment that often has been shielded from the oversight and supervision of parents and other significant adults (Cole et al., 2001). In a medium devoid of standards for conduct and codes of ethics, many young people falter in the quality of their online interactions with others, demonstrating instead a paucity of respect, responsibility, honesty, kindness, justice, or tolerance (Willard, 2000).

**Conclusion**

Technology is the great equalizer in education, and as such, many children have expert knowledge at their fingertips. The more children with the capability to manipulate computers will, in fact, increase the likelihood of damaging acts to computer systems. If digital ethics are not taught, and challenge and excitement are not found in our schools, the cyber world will continue to be a accepting and exciting space for children. The ethical message needs to be embedded in our own educational technology. Our teachers need to be technology leaders in their respective schools and communities, rather than the children. Parents need more technology training to be able to understand what children are doing with the technology. School leaders must understand the legal issues and perils, and implement proper policies and procedures to protect the wellbeing of their school districts. The message of computer ethics needs to start early and be continually reinforced at every level.

**References**

WHAT ROLE DOES EDUCATION PLAY


