

Hacking, Cracking and Juvenile Behavior

Kathy Weise

Lesley University

ECOMP 6101 Online

January 10, 2006

Abstract

Hacking is widely known as utilizing computer and internet resources without permission for illegal activities. Many hackers do not condone illegal activities but there are certain cultural traits and an online community of sharing that exists and is readily available to anyone with unfiltered internet access. The costs of illegal hacking activities are tremendous to the world economy. Students need to be taught appropriate use of technology and guided to suitable and constructive activities.

"Hacker is a term used to describe people who create and modify computer software and computer hardware." (Wikipedia, 2006) Within the online hacking culture, the term refers to people skilled in computer programming, administration and online security. The term "Cracker" has been coined to designate those who utilize these skills to partake in illegal activity. The hacker culture started back in the 1960's and has taken credit for building the Internet, expanding and disseminating the Unix operating system, running Usenet and supporting the continuing operation of the World Wide Web. (Raymond, 2001)

This online hacking culture has developed into a unique community that freely shares information and prides themselves in sharing not only technical programming aptitudes and abilities but also philosophies that are anti-establishment and the belief that information should be free, uncensored and shared. (Trigaux, 1998) Goldstein, editor of 2600: The Hacker's Quarterly, states that "It's all about technology, the thrill of discovery, and sharing information." (CNN/Goldstein, 2001) MIT Hacking Ethics states that the goal is to discover and learn, not to steal, destroy or invade anyone's privacy. (MIT, 2005) Not all hacker's have legal motives, but many do. The media reports more on the illegal activities and thus many people believe that hacking is inherently illegal which is not the case.

Technology provides elements that allow people who use it to behave differently than they do in the 'real world'. It creates the illusion that the internet user is anonymous, it reduces social and contextual cues and tangible feedback, it provides communities that have social norms that may not be appropriate for students, and it allows users to establish multiple identities. (Willard, 2004) Because of the perceived anonymity of the Internet, students may not feel the same sense of guilt and wrongness which they would if the act was physically observable. (Fitzer, 2002)

It is common that children aged 15-20 are particularly attracted to the hacker community. Most kids today know much more about computers than each previous generation and they start playing around online as many have powerful personal computers and fast internet access in their homes and schools. (CNN/Palmer, 2001) The media often portrays hackers in a glamorous light. (Stone, 1999) In an interview with Gary McKinnon, a hacker that got caught on Pentagon computers and now faces 70 years in prison, he claims he saw the movie WarGames and thought, "Could I really do this?" and so in 1995 he tried and was eventually caught. (The Guardian, 2005) There are several big-name hackers, including Steve Wozniak, Bill Gates and Linus Torvalds, who are now highly respected in the technology world, but started and practiced in the underground of hacking. (Symantec, 2005) Particularly in the teenage years, there is a sub-culture of coolness in inappropriate behavior.

(Messmer, 2005) This global community of information provides access to technical and programming information and sharing but also access to chat rooms, newsgroups, and websites containing information on identity falsification, credit card and check fraud, and illegal hacking activities.

(Bowker, 2005)

The range of activities of hackers goes from writing and sharing open source software that is available to everyone for free to criminal activities that are increasingly designed to steal money, credit information and personal identity information. Hackers create and share viruses, worms, malware, spyware, botnets, and programs that allow unauthorized intrusions. (Naraine, 2005) Many hacker attacks go unreported because companies want to avoid negative publicity. The cost of dealing with these interferences affects all companies, public institutions, schools, libraries, homes and everywhere computers are used. The threats of cyber-terrorism targeting electric power and telephone networks, air traffic control systems or the Federal Reserve network indicate that interfering with any of these systems could paralyze the country. (Trigaux, 1998)

School, parents and the community must teach and encourage ethical behavior. The rules and morals change as the technology changes so it is important to be vigilant and adaptive. Harvey, in *Computer Hacking and Ethics*, states there are two strongly opposed approaches to controlling computer education: first, control of the technology and

second, moral training. He advocates empowerment in computer education by providing a culture for young computer enthusiasts to grow. He recommends we provide serious adult models, access to real power by providing access to technology and access to ideas, access to challenging problems and the expertise to guide them, and provide a safe arena for moral experimentation. (Harvey, 1985) Schools need to clearly establish guidelines for acceptable use and clearly delineate repercussions for breaking those rules. Students and staff need to be instructed about hacking and the possible consequences of certain activities. Teachers and parents need to be aware of computer activities and be vigilant to possible hacking behavior. (Stone, 1999) Students need to be guided toward positive and productive activities that will engage and challenge them. There are many opportunities in writing, modifying, documenting and administering open source software programs that can provide a suitable venue for students interested in learning more about computer technologies.

- Bowker, Arthur L. (2005) Guidance Channel Ezine: Advent of the Computer Delinquent. Retrieved June 20, 2005 from <http://guidancechannel.com/default.aspx?index=407%20&cat=18>
- CNN/Goldstein (2001) Q&A with Emmanuel Goldstein of 2600: The Hacker's Quarterly. Retrieved October 23, 2005 from <http://www.cnn.com/TECH/specials/hackers/qandas/goldstein.html>
- CNN/Palmer (2001) Q&A with IBM's Charles Palmer. Retrieved October 23, 2005 from <http://www.cnn.com/TECH/specials/hackers/qandas/palmer.html>
- Fitzer, Kim (2002) Worms, DDos and Cyber-Terrorism. Retrieved June 20, 2005 from <http://students.ed.uiuc.edu/ykelsey/edpsy399/viruses.htm>
- Harvey, Brian (1985) Computer Hacking and Ethics. Retrieved January 8, 2006 from <http://www.cs.berkeley.edu/~bh/hackers.html>
- Messmer, Ellen (2005) NetworkWorld K-12 schools fight to stymie kid hackers. Retrieved October 23, 2005 from <http://www.networkworld.com/news/2005/032105-hacker-kids.html>
- MIT Hacking Ethics (2005) Retrieved January 8, 2006 from <http://www.lysator.liu.se/mit-guide/lame.html>
- The nerd who saw too much (2005) The Guardian. Sydney Morning Herald. Retrieved October 23, 2005 from

<http://www.smh.com.au/news/technology/geek-tragedy-hacker-faces-70year-term/2005>

Raymond, Eric Steven (2001) How to Become a Hacker. Retrieved June 6, 2005 from <http://www.catb.org/~esr/faqs/hacker-howto.html>

Stone, David M. (1999) Computer Hacking. Retrieved January 8, 2006 from <http://www.lrs.ed.uiuc.edu/wp/crime/hacking.htm>

Trigaux, Robert (1998) Hackers – The underbelly of cyberspace. St. Petersburg Times. Retrieved June 20, 2005 from http://www.sptimes.com/Hackers/underbelly_of_cyberspace.html

Trigaux, Robert (1998) Hackers – Computer security's rock 'n' roll pioneer. St. Petersburg Times. Retrieved June 20, 2005 from <http://www.sptimes.com/Hackers/monhackercover.html>

Willard, Nancy (2004) I Can't See You – You Can't See Me: How the Use of Information and Communication Technologies Can Impact Responsible Behavior. Retrieved January 8, 2006 from <http://responsiblenetizen.org/cyberbullying/docs/disinhibition.pdf>