# AAE-190
# Introduction to Aerospace Engineering
# Fall, 2000

## Cyber Ethics and Cyber Crime

(http://www.cybercitizenpartners.org/default.htm)

**"We are in a horse race with kids who have grown up computer skills and teenage ethics" New York Times, April 23, 2000**

**A recent poll of 47,235 elementary and middle school students conducted by Scholastic, Inc. revealed that 48% of kids do not consider hacking a crime.**

**Cyber Ethics: Applying Old Values to a New Medium**
(http://www.cybercitizenship.org/ethics/)

An old adage tells us "Character is what you do when no one is watching."

So it is with the Internet. Online, people can feel invisible and capable of doing things they normally wouldn't do in person or in public – things that they know might be wrong. As the Internet becomes an indispensable tool for everyday life, it is more important than ever to dust off the concept of "citizenship" and apply it to the online world.

Relatively new terms, "cybercitizenship", "cyber ethics", and "netiquette" refer to responsible cyber social behavior. These terms refer to what people do online when no one else is looking. As our kids go online in increasing numbers, cyberethics is a critical lesson, especially since poor e-habits can start at an early age. Unfortunately, we are learning all to well that children armed with computers can be dangerous and cause serious damages and harm, regardless of whether they are trying to be mischievous or intentionally commit cybercrimes.

The Computer Ethics Institute offers the Ten Commandments of Computer Ethics to help reinforce acceptable online behavior.

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that insure consideration and respect for your fellow humans.

**What is Cyber Crime?**

(http://www.cybercitizenship.org/crime/index.html)

Parents, teachers, non-profits, government, and industry have been working hard to protect kids online. However, we also need to think about protecting the Internet from kids who might abuse it.

The Department of Justice categorizes computer crime in three ways:

1. The computer as a target * attacking the computers of others (spreading viruses is an example)
2. The computer as a weapon * using a computer to commit "traditional crime" that we see in the physical world (such as fraud or illegal gambling).
3. The computer as an accessory * using a computer as a "fancy filing cabinet" to store illegal or stolen information.

Reports of alleged computer crime have been a hot news item of late. Especially alarming is the realization that many of the masterminds behind these criminal acts are mere kids. In fact, children no longer need to be highly skilled in order to execute cyber crimes. "Hacker tools" are easily available on the Net and, once downloaded, can be used by even novice computer users. This greatly expands the population of possible wrongdoers. Children (and in some cases - their parents) often think that shutting down or defacing Web sites or releasing network viruses are amusing pranks. Kids might not even realize that what they are doing is illegal. Still other kids might find themselves hanging out online with skilled hackers who share hacking tools with them and encourage them to do inappropriate things online. Unfortunately, some of these kids don't realize that they are committing crimes until it is too late. Even more distressing and difficult to combat is the fact that some in the media portray the computer criminal as a modern day Robin Hood. Nothing could be further from the truth.

So what are cyber crimes? Can the law enforcement authorities find criminals online? How can you create context for your children to understand what cyber crimes are? The following information (and areas throughout the site) will help familiarize you with unethical and illegal online behavior. Additionally, to learn more about cyber crime, visit the Department of Justice Computer Crime & Intellectual Property Section's website at www.cybercrime.gov. The Computer Emergency Response Team (CERT) at www.cert.org and the National Infrastructure Protection Center at the FBI at www.nipc.gov provides regularly updated information and descriptions of cyber crimes.

Following are examples to help parents better explain the scope of seriousness surrounding cyber crimes:

**Inappropriate e-mails**

Just as it is illegal to threaten, harass or stalk others in person, e-mail should be no exception for these acts. E-mail can create a shield of anonymity for the computer user, making communication seem less impactful. Upon first becoming acquainted with e-mail use, children should learn proper communication "tone." Additionally, kids can be exploited by e-mail scams that might lure them into illegal activities that involve hacking, distribution of counterfeit products and the like.

**Hacking**

Hacking, breaking into, or "cracking" refers to manipulation of or intentional damage to another computer or computers. Hacking can take a variety of forms, from cracking computer codes and stealing classified information to vandalizing a Web site.

Illegal entry into a computer system can create a virtual avalanche of destruction, causing serious consequences. Computer viruses are infiltrating computers systems across the country at an ever-increasing rate. If a virus were disable the computer network of a hospital, it could shut down medical instrumentation systems that control life support and monitoring functions-all of which could cost a patient his or her life.

Almost every sector of the economy -- from transportation and financial transactions to emergency services and power distribution -- depends on computers. Disruption of any or all of these operations can result in consequences ranging from monetary losses to catastrophic loss of life.

**Counterfeit and pirated goods**

The Internet is a useful and convenient tool that allows people to find almost anything they want, including products and services that belong to others. Most of us know that we should not go into a store and take software, movies, or CD, without permission. It can be just as wrong, however, to take music or software from the Internet without the permission of the copyright owner.

It is easy to understand why the theft of an object is wrong; it is more difficult for children to understand the concept of theft of intellectual property. It is important that we

teach our kids that they should not download pirated or counterfeit material. They should not download otherwise copyrighted works without permission. There are many websites where the authors of material encourage downloading. It is not wrong to download from these sites. Many others do not. Parents may want to try to learn more about copyright and trademark laws to learn if their kids are behaving ethically. Two places to learn more information are the Department of Justice at www.cybercrime.gov and the U.S. Copyright office at www.copyright.gov/copyright/.

One way that people share counterfeit and pirated goods on the Internet is at "warez" sites. Even though they don't have permission to do so, these websites share copies of software, movies, music, and other goods at discounted rates, or sometimes, even for free. Those who set up and use such sites can find themselves in trouble with the law or being sued by the companies who own the rights to the goods being offered on the site.

**Claiming other's online content or designs as your own**

It is important to teach kids that drawings or content from Web sites are ideas that belong to someone else. Copying these for use in a school project or paper assignment without a reference to where they came from is plagiarism. This is just the same as if your child stole a classmate's homework assignment and tried to turn it in as his/her own. Any use of materials or artwork should be cited appropriately.

**Denial-of-service attacks**

Imagine if you couldn't get to work one morning because someone had blocked the tunnel or bridge you need to cross to get there. You and thousands of others would be stuck on one or the other side, unable to attend to all the things you do every day at your job. This is like what happened to CNN, Yahoo!, eBay and other Web sites that were victim to "denial-of-service" attacks when their Web sites were closed down by hackers.

## Quick Quiz

(http://www.cybercitizenship.org/index.html)

**Is it illegal to download copyrighted material from the Internet without permission of the copyright holder?**

There are times when the downloading of copyrighted material is perfectly legal and even encouraged. More often it is not. Simply because the technology allows you to do it effortlessly does not make it right to do so. Intellectual property, in the form of music, books, pictures and movies is often created by people have worked hard to create the entertainment and/or art that we enjoy.

Unauthorized appropriation of these works can be both unethical and illegal. Be sure that you and your children clearly understand the requirement for permission before they are allowed to download. Read the terms and conditions of the license agreement on the site that you are accessing. If none exist - be wary, get more information and ask questions.

**Is it illegal to tamper with someone's e-mail or deface a web site?**

Tampering with paper mail is illegal; tampering with email is certainly unethical and potentially illegal as well. The fact that the medium has moved from analog (writing) to digital (bits) does not change the nature of the act. Most kids would not consider reading, altering or destroying a letter. The same behavior is applicable to email.

Websites are the work of individuals, businesses and governments. They require considerable effort and often-considerable expense to produce and maintain. A website may be an integral part of a business strategy or communications scheme. Loss and/or repair of the site may involve substantial expense, may be hurtful to a "community" and, in some cases, may jeopardize the nation's infrastructure or national defense. This is an act of vandalism. Defacing real property is not tolerated; online vandalism should not be either.

## Additional Resources

Internet Rules of the Road http://www.usdoj.gov/kidspage/do-dont.htm

The National Infrastructure Protection Center (NIPC) http://www.nipc.gov/

Legal Issues from NIPC http://www.nipc.gov/legal/legal.htm

Information Technology of America http://www.itaa.org/