I. What is a Computer Crime?

a. Criminals Can Operate Anonymously Over the Computer Networks.

1. Be careful about talking to "strangers" on a computer network. Who are these people anyway? Remember that people online may not be who they seem at first.

Never respond to messages or bulletin board items that are:



- Suggestive of something improper or indecent;
- Obscene, filthy, or offensive to accepted standards of decency;
- Belligerent, hostile, combative, very agressive; and
- Threaten to do harm or danger towards you or another

2. Tell a grown-up right away if you come across any information that makes you feel uncomfortable.

3. Do not give out any sensitive or personal information about you or your family in an Internet "chat room." Be sure that you are dealing with someone you and your parents know and trust before giving out any personal information about yourself via e-mail.

4. Never arrange a face-to-face meeting without telling your parents or guardians. If your parent or guardian agrees to the meeting, you should meet in a public place and have a parent or guardian go with you.

b. Hackers Invade Privacy
1. Define a hacker.

A hacker is someone who breaks into computers sometimes to read private e-mails and other files.

2. What is your privacy worth?

What information about you or your parents do you think should be considered private? For example, medical information, a diary, your grades, how much money your parents owe, how much money your family has in a savings account or in a home safe, and your letters to a friend.

Would this kind of invasion of your privacy be any different than someone breaking into your school locker or your house to get this information about you and your family?

c. Hackers Destroy "Property" in the Form of Computer Files or Records. 
1. Hackers delete or alter files.

2. When you write something, like a term paper or report, how important is it to be able to find it again?

Would this be different if someone broke into your locker and stole your term paper?

3. How important is it that data in computers like your term paper, a letter, your bank records, and medical records, not be altered?

How important is it for a drug company or a pharmacy to not have its computer files altered or deleted by hackers? What would happen if a hacker altered the chemical formulas for prescription drugs, or the flight patterns and other data in air traffic control computers? What does the term "tamper" mean? To interfere in a harmful way or to alter improperly.

Is tampering with computer files different from tampering that occurs on paper files or records?

 **Glossary**

d. Hackers Injure Other Computer Users by Destroying Information Systems 
1. Hackers cause victims to spend time and money checking and resecuring systems after break-in. They also cause them to interrupt service. They think it's fine to break-in and snoop in other people's files as long as they don't alter anything. They think that no harm has been done.

2. Hackers steal telephone and computer time and share unauthorized access codes and passwords. Much of the stealing is very low-tech. "Social engineering" is a term used among crackers for cracking techniques that rely on weaknesses in human beings rather than on software. "Dumpster diving" is the practice of sifting refuse from an

office or technical installation to extract confidential data, especially security compromising information.

Who do you think pays for this? How much stealing of computer time do you think there is? For example, there is $2 billion annually in telephone toll fraud alone. Would you want someone going through your garbage? Have you ever thrown away private papers or personal notes?

3. Hackers crash systems that cause them to malfunction and not work.

How do we use computer information systems in our daily lives? What could happen if computers suddenly stopped working? For example, would public health and safety be disrupted and lives be endangered if computers went down?

 **Glossary**

e. Computer "Pirates" Steal Intellectual Property.
1. Intellectual property is the physical expression of ideas contained in books, music, plays, movies, and computer software. Computer pirates steal valuable property when they copy software, music, graphics/pictures, movies, books (all available on the Internet).

How is the person who produced or developed these forms of entertainment harmed? Is this different from stealing a product (computer hardware) which someone has invented and manufactured? Who pays for this theft?

2. It may seem simple and safe to copy recordings, movies and computer programs by installing a peer-to-peer (P2P) file sharing software program. However, most material that you may want to copy is protected by copyright which means that you are restricted from making copies unless you have permission to do so. Making copies of intellectual property-including music, movies and software--without the right to do so is illegal. P2P software and the files traded on the P2P networks may also harm your computer by installing viruses or "spyware," or allow others to access the files contained on your hard drive beyond those you intend to share.

3. Copyright violations have civil and criminal remedies.

a.) Civil remedy: copyright holder can sue infringer for money to cover loss of sales or other loss caused by infringement.

b.) Criminal remedy: jail or fine paid to the government (not copyright holder) where person infringes a copyright for commercial advantage or private gain. For example, a person who makes multiple copies of a video, and sell the copies.

 **Glossary**

II. How Can We Prevent Computer Crime?

a. By Educating Everyone.

For example, users and systems operators; people who hold personal data and the people about whom it is held;

people who create intellectual property and those who buy it; and the criminals.

We must educate people to:
1. Understand how technology can be used to help or hurt others.

2. Think about what it would be like to be the victim of a computer hacker or computer pirate.

b. By Practicing Safe Computing.
1. Always ask: Who has or may have access to my log-in address?

2. Remember: People such as computer hackers and pirates who hurt others through computer technology are not "cool." They are breaking the law.

c. Code of Responsible Computing.
1. Review the Code of Responsible Computing and have the students sign it as their pledge to use the computer in an ethical manner.

2. Find additional suggestions for the classroom on appropriate computer use and manners (see links below), check out the Computer Learning Foundation's Strategies for Teaching Responsible Computing.