Model Lesson Plan

Topic: Cyber-crime
Created by: Caitlin Wilson
Date:
Sources: U.S. Dept. of Justice, Cyber-ethics for Kids, *available at* http://www.usdoj.gov/criminal/cybercrime/rules/lessonplan1.htm;
Gregg R. Zegarelli. Computer Fraud and Abuse Act of 1986, Computer Science Study Guide *available at* http://www.bookrags.com/sciences/computerscience/computer-fraud-and-abuse-act-of-198-csci-01.html.
Hackers (1995)
Time: 50 minutes

I. GOALS

a. This lesson will introduce students to the criminal implications and consequences of computer crime, specifically hacking.

II. OBJECTIVES

a. Knowledge Objectives
    i. As a result of this class, students will be better able to:
        1. know what types of Internet activity are or should be considered criminal;
        2. understand how criminal prohibitions against certain types of Internet activity are best implemented in law.
b. Skills Objectives
    i. As a result of this class, students will be better able to:
        1. determine whether computer crimes are unique and require their own legislation or whether they are just "updated" versions of traditional crimes;
        2. determine whether their own computer activity or that of their peers could be considered criminal.
c. Attitude Objectives
    i. As a result of this class, students will be better able to feel:
        1. their actions and the actions of their peers, especially regarding Internet activity, can and will have real consequences.

III. CLASSROOM METHODS

a. **Opening discussion** (5+ minutes)
b. Start discussion by asking:
    i. What comes to mind when you hear the term computer crime?
        1. Pirating music, software; child pornography; identity theft

ii. Do you think these types of actions constitute completely new crimes or do you think they are just "updated" versions of other crimes? Why?
iii. How would you feel if someone hacked into your email and read your personal messages? How would you feel if someone hacked into the school computers and had access to personal information about you, like your grades?

c. **Film Clip** (10 minutes)
   i. How relevant is computer crime to people your age?
      1. Show opening sequence from the film *Hackers*, which features the U.S. Secret Service using excessive force to raid the home of an eleven year old, who has written a virus that was unleashed and crashed 1507 computer systems.
d. **Discussion** (2 minutes)
   i. This movie is dated, however, teens have historically been linked to computer crimes, causing problems both then and now:
      1. 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.

e. Case Study (20 minutes)
   i. Modified fact pattern attached.
      1. Press Release regarding Massachusetts Teen Convicted for Hacking into Internet and Telephone Service Providers and Making Bomb Threats to High Schools in Massachusetts and Florida (September 8, 2005) is available by the following link: www.cybercrime.gov/juvenileSentboston.htm.
   ii. Have students count off in groups of four.
   iii. Distribute fact pattern to groups.
   iv. Read the fact pattern aloud**.**
   v. Let students work in groups to determine what "crimes" Henry has committed (traditional crimes or computer crimes?) and what they feel the consequences for those crimes should be.
   vi. Have groups report back to entire class.
   vii. Record ideas on board, both ideas for what crimes Henry has committed and what his punishment should be.
      1. For example, Henry could be guilty of trespass and theft as well as hacking.
   viii. Inform class what "really" happened in the case of "Henry" (see press release)
   ix. Ask class whether the law should treat traditional crimes committed via computer differently.

f. **Explanation of Law with Overheads** (10 minutes)
    i. There are both state and federal laws which deal specifically with computer crime and there are laws which are not exclusively directed toward the Internet including laws relating to child pornography, threatening communications, fraud and intellectual property, that have been used to adjudicate cyber crimes.
    ii. Introduce Statutes
        1. State Laws
            a. Malicious Mischief Statute, RCW 9A.48.70, .80, .90, .100
            b. Computer Trespass Statute, RCW 9A.52.110, .120, .130
        2. Federal Statutes
            a. Computer Fraud and Abuse Act, 18 U.S.C. §1030 (as amended by USA Patriot Act)
                i. Depending on time, determine how in-depth discussion of these laws will be.

g. **Wrap-Up**
    i. The most important points to take away from today's class are that the government recognizes computer crimes, including hacking, can be serious criminal offenses, even leading them to create laws that specifically deal with computer crime and teens can be penalized harshly for their misuse of computers.

IV. EVALUATION

a. Participation in class discussion.
b. Group participation in case study.
c. Homework assignment.

V. ASSIGNMENT

a. Students should develop their own code of cyber-ethics with provisions for both public and private use computers. They should incorporate their own beliefs about how computers should be used in light of the pertinent laws.
See http://www.cybercrime.gov/rules/acceptableUsePolicy.htm for example.

Henry the Hacker[1]

In March 2004, a high school student, "Henry" sent an e-mail to a Florida school with the caption, "this is URGENT!!!" The text of the e-mail read:

"your all going to perish and flourish...you will all die
Tuesday, 12:00 p.m.
we're going to have a "blast"
hahahahahaha wonder where I'll be? youll all be destroyed. im sick of your **[expletive deleted]**
school and piece of **[expletive deleted]** staff, your all gonna **[expletive deleted]** die you pieces of crap!!!!
. . . "

As a result of this bomb threat, the school was closed for two days, while a bomb squad, canine team, the fire department and Emergency Medical Services were called in. In August 2004, Henry logged into the Internet computer system of a major Internet Service Provider ("ISP") using a program he had installed on an employee's computer. This program allowed him to use the employee's computer remotely to access other computers on the internal network of the ISP and gain access to portions of the ISP's operational information.

In January 2005, Henry gained access to the internal computer system of a major telephone service provider that allowed him to look up account information of the telephone service provider's customers. He used this computer system to discover key information about an individual who had an account with the telephone service. He then accessed the information stored on this individual's mobile telephone, and posted the information on the Internet.

During this same time period, Henry used his access to the telephone company's computer system to set-up numerous telephone accounts for himself and his friends, without having to pay for the accounts.

Also in January, 2005, an associate Henry set-up accounts for the him at a company which stores identity information concerning millions of individuals allowing the him to look at the identity information for numerous individuals, some of which he used for the purpose of looking up the account information for the victim whose personal information he posted on the Internet.

In the spring of 2005, Henry, using a portable wireless Internet access device, arranged with one or more associates to place a bomb threat to a school in Massachusetts and local emergency services, requiring the response of several emergency response units to the school on two occasions and the school's evacuation on one.

In June 2005, Henry called a second major telephone service provider because a phone that a friend had fraudulently activated had been shut off. In a recorded telephone call, Henry threatened the telephone service provider that if the provider did not provide him access to its computer system, he would cause its web service to collapse through a denial of service attack- an attack designed to ensure that a website is so flooded with request for information that legitimate users cannot access the website. The telephone service provider refused to provide the requested access. Approximately ten minutes after the threat was made, Henry and others initiated a denial of service attack that succeeded in shutting down a significant portion of the telephone service provider's web operations.

After all this, Henry was caught. What crimes did Henry commit? What do you think happened to Henry?

[1] Fact pattern modified from press release *available at* http://www.cybercrime.gov/juvenileSentboston.htm

Massachusetts Teen Convicted for Hacking into Internet and Telephone Service Providers and Making Bomb Threats to High Schools in Massachusetts and Florida

www.cybercrime.gov/juvenileSentboston.htm.

Boston, MA... A Massachusetts juvenile pled guilty in federal court and was sentenced today in connection with a series of hacking incidents into Internet and telephone service providers; the theft of an individual's personal information and the posting of it on the Internet; and making bomb threats to high schools in Florida and Massachusetts; all of which took place over a fifteen month period. Victims of the Juvenile's conduct have suffered a total of approximately $1 million in damages.

United States Attorney Michael J. Sullivan for the District of Massachusetts; United States Attorney H. E. Bud Cummins, III for the Eastern District of Arkansas; United States Attorney R. Alexander Acosta for the Southern District of Florida; Steven D. Ricciardi, Special Agent in Charge of the U.S. Secret Service in New England; Kenneth W. Kaiser, Special Agent in Charge of the Federal Bureau of Investigation in New England; William Sims, Special Agent in Charge of the Secret Service in Miami, Florida; and William C. Temple, Special Agent in Charge of the Federal Bureau of Investigation in Little Rock, Arkansas, announced today that in a sealed court proceeding a Massachusetts teenager pled guilty before U.S. District Judge Rya W. Zobel to an Information charging him with nine counts of Juvenile Delinquency.

By statute, federal juvenile proceedings and the identity of juvenile defendants are under seal. The Court has authorized limited disclosure in this case at the request of the government and defendant.

Judge Zobel also imposed a sentence today of 11 months' detention in a juvenile facility, to be followed by 2 years of supervised release. During his periods of detention and supervised release, the Juvenile is also barred from possessing or using any computer, cell phone or other electronic equipment capable of accessing the Internet.

Had the Juvenile been an adult, the underlying charges would have been charged as three counts of Making Bomb Threats Against a Person or Property, three counts of Causing Damage to a Protected Computer System, two counts of Wire Fraud, one count of Aggravated Identity Theft, and one count of Obtaining Information from a Protected Computer in Furtherance of a Criminal Act.

The Juvenile was also charged in an Information in the Eastern District of Arkansas with one count of Juvenile Delinquency. Had the Juvenile been an adult, the underlying charge in the Arkansas case would have been Causing Damage to a Protected Computer System. The case was transferred to the District of Massachusetts and the Juvenile pled guilty to the charge last month. Today's sentence is the result of the Juvenile's guilty plea to both the Massachusetts and Arkansas charges.

"Computer hacking is not fun and games. Hackers cause real harm to real victims as graphically illustrated in this case," stated U.S. Attorney Sullivan. "Would-be hackers, even juveniles when appropriate, should be put on notice that such criminal activity will not be tolerated and that stiff punishments await them if they are caught."

The basis for the charges was a course of criminal conduct that took place over a fifteen month period beginning in March, 2004 when the Juvenile sent an e-mail to a Florida school with the caption, "this is URGENT!!!". The text of the e-mail read:

> "your all going to perish and flourish...you will all die
> Tuesday, 12:00 p.m.
> we're going to have a "blast"
> hahahahahaha wonder where I'll be? youll all be destroyed. im sick of your **[expletive deleted]**

school and piece of **[expletive deleted]** staff, your all gonna **[expletive deleted]** die you pieces of crap!!!!
DIE MOTHER **[expletive deleted]** IM GONA BLOW ALL YOU UP AND MYSELF
ALL YOU NAZI LOVING MEXICAN FAGGOT BITCHES ARE DEAD"

As a result of this bomb threat, the school was closed for two days, while a bomb squad, a canine team, the fire department and Emergency Medical Services were called in.

In August, 2004, the Juvenile logged into the Internet computer system of a major Internet Service Provider ("ISP") using a program he had installed on an employee's computer. This program allowed the juvenile to use the employee's computer remotely to access other computers on the internal network of the ISP and gain access to portions of the ISP's operational information.

In January, 2005, the Juvenile gained access to the internal computer system of a major telephone service provider that allowed him to look up account information of the telephone service provider's customers. He used this computer system to discover key information about an individual who had an account with the telephone service. He then accessed the information stored on this individual's mobile telephone, and posted the information on the Internet.

During this same time period, the Juvenile used his access to the telephone company's computer system to set-up numerous telephone accounts for himself and his friends, without having to pay for the accounts.

Also in January, 2005, an associate of the Juvenile set-up accounts for the Juvenile at a company which stores identity information concerning millions of individuals allowing the Juvenile to look at the identity information for numerous individuals, some of which he used for the purpose of looking up the account information for the victim whose personal information he posted on the Internet.

In the spring of 2005, the Juvenile, using a portable wireless Internet access device, arranged with one or more associates to place a bomb threat to a school in Massachusetts and local emergency services, requiring the response of several emergency response units to the school on two occasions and the school's evacuation on one.

In June, 2005, the Juvenile called a second major telephone service provider because a phone that a friend had fraudulently activated had been shut off. In a recorded telephone call, the Juvenile threatened the telephone service provider that if the provider did not provide him access to its computer system, he would cause its web service to collapse through a denial of service attack- an attack designed to ensure that a website is so flooded with request for information that legitimate users cannot access the website. The telephone service provider refused to provide the requested access. Approximately ten minutes after the threat was made, the Juvenile and others initiated a denial of service attack that succeeded in shutting down a significant portion of the telephone service provider's web operations.

The investigation of the Juvenile's associates is continuing.

The case was investigated by the U.S. Secret Service and the Federal Bureau of Investigation. The Massachusetts case was prosecuted by Assistant U.S. Attorneys Stephen Heymann and Seth Berman in Sullivan's Internet Crimes Unit. The Arkansas case was prosecuted by Assistant U.S. Attorney Karen Coleman in Cummins' Office. The prosecution in Florida was handled by Assistant U.S. Attorney Anita Gay in Acosta's Office.

Press Unit: Samantha Martin, (617) 748-

WASHINGTON LAW

9A.48.070. Malicious mischief in the first degree

(1) A person is guilty of malicious mischief in the first degree if he knowingly and maliciously:

(a) Causes physical damage to the property of another in an amount exceeding one thousand five hundred dollars;

(b) Causes an interruption or impairment of service rendered to the public by physically damaging or tampering with an emergency vehicle or property of the state, a political subdivision thereof, or a public utility or mode of public transportation, power, or communication; or

(c) Causes an impairment of the safety, efficiency, or operation of an aircraft by physically damaging or tampering with the aircraft or aircraft equipment, fuel, lubricant, or parts.

(2) Malicious mischief in the first degree is a class B felony.

VI. 9A.48.080. Malicious mischief in the second degree

(1) A person is guilty of malicious mischief in the second degree if he or she knowingly and maliciously:

(a) Causes physical damage to the property of another in an amount exceeding two hundred fifty dollars; or

(b) Creates a substantial risk of interruption or impairment of service rendered to the public, by physically damaging or tampering with an emergency vehicle or property of the state, a political subdivision thereof, or a public utility or mode of public transportation, power, or communication.

(2) Malicious mischief in the second degree is a class C felony.

9A.48.090. Malicious mischief in the third degree

(1) A person is guilty of malicious mischief in the third degree if he or she:

(a) Knowingly and maliciously causes physical damage to the property of another, under circumstances not amounting to malicious mischief in the first or second degree; or

(b) Writes, paints, or draws any inscription, figure, or mark of any type on any public or

private building or other structure or any real or personal property owned by any other person unless the person has obtained the express permission of the owner or operator of the property, under circumstances not amounting to malicious mischief in the first or second degree.

(2)(a) Malicious mischief in the third degree under subsection (1)(a) of this section is a gross misdemeanor if the damage to the property is in an amount exceeding fifty dollars.

(b) Malicious mischief in the third degree under subsection (1)(a) of this section is a misdemeanor if the damage to the property is fifty dollars or less.

(c) Malicious mischief in the third degree under subsection (1)(b) of this section is a gross misdemeanor.

9A.52.110. Computer trespass in the first degree

(1) A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic data base of another; and

(a) The access is made with the intent to commit another crime; or

(b) The violation involves a computer or data base maintained by a government agency.

(2) Computer trespass in the first degree is a class C felony.

9A.52.120. Computer trespass in the second degree

(1) A person is guilty of computer trespass in the second degree if the person, without authorization, intentionally gains access to a computer system or electronic data base of another under circumstances not constituting the offense in the first degree.

(2) Computer trespass in the second degree is a gross misdemeanor.

9A.52.130. Computer trespass--Commission of other crime

A person who, in the commission of a computer trespass, commits any other crime may be punished for that other crime as well as for the computer trespass and may be prosecuted for each crime separately.

Computer Fraud and Abuse Act, 18 U.S.C. § 1030

The United States Computer Fraud and Abuse Act of 1986 was an amendment to the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. It was the first comprehensive legislation in the United States to identify and provide for the prosecution of crimes committed through and against computer systems. It has since been amended by the USA Patriot Act.

The first person convicted of violating the act was a Cornell computer science grad student named Robert Morris who, in 1988, created an Internet worm (much like in the movie *Hackers*) as an experiment. The worm was not intended to cause malicious harm, however, it resulted in causing computer failure in more than 6,000 computers (which constituted 6% of all computers on the Internet at that time).

U.S. Attorney Frederick J. Scullen, Jr. noted: "Among other things, the *Morris* case should put the would-be hacker on notice that the Department of Justice will seek severe penalties against future computer criminals, whether or not they are motivated by a venal or malicious intent."[2]

[2] Gregg R. Zegarelli. Computer Fraud and Abuse Act of 1986, Computer Science Study Guide *available at* http://www.bookrags.com/sciences/computerscience/computer-fraud-and-abuse-act-of-198-csci-01.html.