INTERNET DEVIANCE 101

The Internet is growing at an unbelievable rate. According to the *New York Times* "over half of all the people who surf the Internet first logged on in 1995." What is amazing is that a few years ago there were no regulations and laws regulating behavior on the Internet. Now, the Internet is going through major changes as the government and other institutions make sure that certain language and items are not available to certain users. But, government regulations of the Internet may not be possible as many of the first users of the Internet are used to free flowing information.

The Computer Emergency Response Team "reported 2,241 'incidents' in 1994, roughly double of the number of break-ins in 1993." This is of course reported incidents and probably not even close to actual incidents. As people become more computer literate and able to understand how the Internet works, people may become more deviant.

Internet deviance is an action that breaks Internet rules and norms; including, but not necessarily, committing illegal acts, ranging from destroying files to netiquette. Netiquette is the *mores and norms* that regulate considerate and appropriate behavior on the Internet; mainly, e-mail.

A necessity to avoid getting caught is to remain a shadow that is untraceable. Anonymity is the goal. People can do whatever they want on the Internet, but without the knowledge to hide their tracks they will more than likely get caught. Hackers spend a great deal of thought and time ensuring that they do not leave any traceable information. And if they do, it must be misleading or points the finger at numerous people; thus, making it difficult to figure out who actually did the crime.

But not all hackers commit criminal acts. Hackers are people who are knowledgeable about computers and able to figure out tough computer problems. A cracker, on the other hand, is the hard core computer criminal who does a lot of damage to systems. Although crackers learn a lot too, mainly this is the goal of the hacker. As a reward, a hacker may obtain pirated software, but the true goal is the challenge and fun in learning more about computers. How do I commit these illegal acts without getting caught? What do I need to know to out smart the system administrator and other authorities? All of these relate to the need to remain “invisible” and a shadow within the telephone cords. Will I be able to get away with it?

Therefore, I am attempting to understand the hacker; instead, of trying to catch the culprit. All of my literature deals with understanding the motivations, goals, and tactics of a hacker in the view of a systems and security administrator. The literature focused on the consequences of the hacker, and labeled that person as a “criminal.” Although a hacker may be destructive, my experience is that, for the most part, a hacker does not care to damage or sabotage anything but to have fun in learning about computers and the Internet.

REQUIRED READINGS

Obtaining sources about Internet deviance was difficult because it is so recent. All, of my sources deal with “computer crime and deviancy” and therefore is related to my topic of Internet deviance.

The main source of information is provided by Hollinger. Hollinger gives an overview of the current articles in the early 1980’s on computer deviance. The article includes ten acts that define computer deviance and hacking. The ten acts are:

1. Acquiring another user’s password.
2. Unauthorized use of someone else’s computer account.
3. Unauthorized “browsing” among another user’s computer files.
4. Unauthorized “copying” of another user’s computer files.
5. Unauthorized file modification.
6. Deliberate sabotage of another user’s programs.
7. Deliberately “crashing” a computer system.
8. Deliberate damage or theft of computer hardware.
9. Making an unauthorized or “pirated” copy of proprietary computer software for another user.
10. Receiving an unauthorized or “pirated” copy of computer software from another user.

In many aspects, many of the ten are similar to what the hacker’s I interviewed have done, but with the Internet. Lastly, this article attempts to define the differences of people who commit computer deviance. There are the Pirates, or people who “give or receive illegally copied versions of popular software programs.” There are the Browsers, or people who “gain occasional unauthorized access to another user's university computer account and browsed the private files of others." Finally, there are the Crackers, or people who "copied, modified, and sabotaged other user's computer files and programs."

The next source of information is from the Chantico Publishing Company. The Chantico Publishing Company, Inc. tried to define the "characteristics of the computer criminal." For the most part, this reaffirms that computer criminals are generally young white males. Although the book reports that females are beginning to hack it is still disproportionately male dominated. Moreover, this book tries to explain the motivational factors of why people become hackers. The four are "resentment...a sense of gaming...challenge...and financial gain." Resentment is defined as "a computer crime that is a person's way of striking back and to gain recognition." A sense of gaming is defined as "playing against the security manager and the software in place to prevent access becomes a game." Challenge is defined as "a person seeing his/her position as me versus them and enjoys the mental effort required to crack a system." Finally, financial gain is defined as "financial motivation."

Pfuhl attempted to explain why "computer crime, abuse, and hacking" are wrong and harmful. For the most part, he argues that this is harmful because it hurts property and business. Moreover, he explains that recent laws passed are not enough to deter people from committing computer deviancy because many people do not see "computer crime" as bad. Most people associate computer criminals as "good people" and not "violent," therefore, are not as bad as "real criminals." This is one of the reasons why many of the advisors do not feel that Internet deviance is wrong. Lastly, Pfuhl explains that "hacking" is a "game." The goal is to get into systems without getting caught.

Parker is the next most important source of information. Parker explains various unauthorized entrances and explains what to look for. Moreover, he attempts to analyze who the perpetuator is, in order, to know who to focus on in trying to catch computer criminals.

Bequai focused on the lack of deterrence of computer criminals. He believes that this is a white collar crime and as a result, many people do not pay as much attention because it is not a “true crime.” Laws enacted to prosecute illegal computer activities are lenient when computer criminals are sentenced. One reason is that a hacker can provide valuable security knowledge to a company. Another reason, as already mentioned, many people do not feel that hackers are harmful to society.

Finally, Marx is a source on netiquette, or in his words, “humanware.” He explains that “new technologies require new manners” and that e-mail is especially vulnerable to “interception by third parties.”

> New opportunities and temptations for deception and rudeness are provided by technologies that offer remote access and anonymity. The absence of visual or auditory cues makes it easier to conceal, deceive, and manipulate. The isolated individual sending messages at a computer terminal or responding to the requests of an electronic voice may make it hard to remember that there is (or will eventually be) a human being at the other end. The emotionless quality of the medium, the invisibility of the other, and the anonymity of the sender are not inherently conducive to civility.

Marx’s attempt to explain the ease in which deviancy can be done on the Internet can also be found in my research setting.

Methods

I am the Assistant Supervisor at a computer lab on campus and thought that studying where I worked would be beneficial because I am there at least thirty hours a week. This obviously brought a lot of advantages and consequences to my research project. One of the advantages is that I am familiar with my co-workers. The following is a description of the advisors at the computer lab.

Deckland, the Supervisor, has been here for at least four years. He is a white male, middle class and up, Catholic, and politically conservative. Although he is a graduate student in the department of Telecommunications he hates computers and technology. He feels that computers are going to destroy the world and if it was not for the money he would be a fireman.

The next person in line is Herb, the “Senior Advisor.” He is a white male, middle class and up, majoring in Finance and Information Systems, and considers himself a Libertarian; in other words, the government should not intervene as much in people’s affairs.

Tom is the next advisor on the totem pole. He is a white male, middle class, majoring in Information Systems, and I am not sure about his political affiliation. He is the most interesting in terms of his interaction with users because he can be condescending and temperamental.

Mark, is a white male, middle class and up, Catholic, majoring in Information Systems, and politically in the "middle." This is one of the people I interviewed because I felt that he, by my definition, is a "hacker." In other words, he will spend countless hours trying to figure out a computer/Internet problem.

The next advisor is Henry, he is a white male, middle upper class and up, majoring in Marketing, and conservative. Henry can be pretty weird and obnoxious because he does or says things that are pretty random.

Zeke is a white male, middle class, majoring in Chemistry and Biology, and is apolitical. He is a smart person, who knows how to manipulate and figure out problems with computers. We briefly talked about computer and Internet deviance.

Elizabeth is a Chinese female, middle lower class, majoring in Information Systems. She is generally the focus of all put downs by the male advisors. I think this is due to her language barrier and that she sort of understands what is being said.

On the other hand, Jill is generally left alone because she does not understand the jokes directed at her. For this reason, not many advisors make fun of her because it is no fun. Jill is a Malaysian female, I cannot tell her class or political orientation, and she is majoring in Information Systems.

The last two advisors are Don, and Jim. I do not really know these two because they are recent hires, and I do not work with them; therefore, do not talk with them that often.

There are two former advisors, Kant and Tim, that I interviewed. Kant is a white male, middle class an up, and I am not sure what his political and religious affiliation is. Tim, is a white male, middle class and up, and again I am not sure what his political and religious affiliation is. Both of these people represent what many people would consider as the stereotypical "hacker."

I gained entrée by notifying all of the advisors through electronic-mail (e-mail). Sending a message to the advisor's e-mail list, I explained to them that I wanted to study the lab and that if anyone objected they should let me know. This was a quick and efficient way of getting to all of the advisors, and nobody objected to. The only person I talked to in person was the Supervisor because I wanted to get his okay first.

Another advantage in studying the lab is that I am familiar with its setting. The lab is split into two converted classrooms with the lab office in the middle. Room 107 has computers arranged for more individual work. There are eight mini-rows of computers with each computer sitting in a cubicle like work study (similar to the individual work stations in Norlin). Then there is a row of ten computers that string against the wall across the room, from entrance to the fire exit. There is a dot matrix printer that sits in the back of the room, and two laser printers in the front of the room. Because there are more computers in this room, mostly individuals work here. Moreover, if people are to work in groups it generally means that the congregation of people and chairs around the computer will block the walkways in that room.

On the other hand, room 104 has more spacing and is more conducive to group work. Similar to room 107 there are a string of computers from the entrance to the fire exit; but, is different in that there is one computer for every two or three cubicles. Moreover, instead of eight mini-rows there are three long-rows of computers. Thus, giving students more space to work with. Lastly, all three printers sit in front of the room.

But being a participant observer brought some ethical and methodological problems. One of the major problems I experienced is disclosure. Should I tell the advisors the focus of my research? Am I ruining friendships or work relationships? Am I using them for my own personal and academic gains? Moreover, Internet deviance, especially software piracy and other illegal activities, brought out ethical concerns. Mainly, this stems from Professor Leo's lecture about his own research and ethical dilemmas. Although I do not feel that I will ever be subpoenaed by a court of law because of this paper I cannot but wonder what if I am? Other concerns are am I breaking the law by observing people break laws?

These ethical concerns also brought methodological problems. Should I protect an advisor if s/he commits an illegal act? As a result, is my data tainted because I am not reporting the "whole truth and nothing but the truth." For the most part, I ignored many of these concerns and did the best I could in recording what I saw.

I was obviously sympathetic to the advisors; especially, those who committed Internet Deviance that I benefited from. For example, a game on the advisor's computer is Duke Nuke'm 3D. This game is a shareware version, but, after fifty uses becomes a copyright violation. So far we have played the game at least ninety times.

In a sense, I am already a "native." This is another methodological problem I faced because the information I gathered may be tainted as I agreed with the advisors with what they were doing. There was not a case of Internet deviance that I might not have done. Moreover, I am committing Internet deviance every time I access that shareware game.

For the most part, the bulk of my data comes from observations while at the lab. Watching advisors, I began noticing forms of deviancy on the Internet, making my topic more refined and focused. Although I worked thirty plus hours a week at the lab I probably spent ten to fifteen hours (give or take a couple hours) from observing people and the lab. This is partly because I had duties to perform; for example, helping students with computer problems, general lab stuff (cleaning up, putting paper in the printer, etc.).

Because the lab sits in the center of the computer lab I thought that I would give myself another perspective by moving around in the lab and trying to notice things that I would otherwise would not. Unfortunately, I did not notice any forms of deviance performed by users at the lab. Thus, I mainly focused on the advisors for my information. Moreover, most of the advisors will disclose what they are doing and feeling; while users who are committing Internet deviance will avoid me because I am in a position of authority and might report them. Also, if I walked up and down the rows of computers, it might make a person nervous. As a result, I focused on the advisors because they would not care if they disclosed sensitive information about illegal activities on the Internet.

The rest of my information came from interviews. I interviewed advisors and former advisors who I thought were computer and Internet literate, and also who have committed some sort of deviancy on the Internet. I interviewed four people. All four are white males, in their early twenties, and in the middle-class or up. Two were former advisors and two are current ones. This may bring interesting biases as there were no women I interviewed, nor people in different racial and ethnic groups. For the most part, people who are computer literate and are "hackers" are white males, in their early twenties, and in the middle-class. Lastly, I never saw any of the female advisors commit any Internet deviance. This could be because they might not have the knowledge to do so, but, I feel that "hacking," is done exclusively by males.

The interviews were carried out in an extremely casual manner. One of the interviews was done while eating lunch at Taco Bell. Another interview was done in a lounge at the Business School. Another interview was done while we both were working. And the last interview was done in a club office at the Business School. For the first three interviews I would transcribe the conversation shortly after it was done. But for the last one, due to time constraints, I could not transcribe it until three days later. All four interviews lasted about thirty to forty-five minutes. I did not have any recording devices because I did not feel that it was appropriate in a setting such as Taco Bell. Moreover, I tried not to lead the interviewees by making it a conversation. I am sure, without realizing it, that I had leading questions; but, I felt that the interviews were conversational. The only problem with Taco Bell, as a setting for an interview, is that the conversations were broken up during bites of food. Other than that, I felt that the interviews went well.

After coding my field notes, the bulk of my information indicated that my topic should be either politics of the lab or Internet deviance. I am more interested in Internet deviance, therefore, picked it over politics. Having a predetermined topic could have happened as I was thinking about studying the Internet for my research project; however, I did not notice any forms of Internet deviance until after four weeks of field notes.

Moreover, I would have never thought of shareware violations as illegal until after further thought instigated by my research. Also, I knew that Internet deviance occurs, but, I never knew at what extent. Again my research focused only at the computer lab and I found that Internet deviance is prevalent.

Because I am studying Internet deviance, I thought I would conduct some of my research on the Internet. Using search engines I searched for articles under words such as hacking, and deviance. There were a bunch of information on hacking, but not what I wanted. Deviance was an empty search also. I did stumble upon some good *New York Times* articles that dealt with basic Internet statistics and a world renowned hacker named Kevin Mitnick. And I found policies relevant to social control.

The best page I went to, however, is the Candyman site. This site is illegal because the content deals with how to pirate software, steal money from ATM's, make bombs, etc.; and also, uses other people's sites to store their home page. The Candyman site moves every week once his/her site is discovered.

I also went to a talk relevant to my topic at the Conference on World Affairs.

Lastly, some of my information is not entirely from this semester. Most of the more "hard-core" hacking is from observations a year or a couple of years ago. But, for the most part, my information is from this semester.

Findings

Throughout my data there were underlying motivations to commit Internet deviance. Again Internet deviance is an action that breaks Internet rules and norms; including, but not necessarily, committing illegal acts, ranging from destroying files to netiquette. Netiquette is the *mores and norms* that regulate considerate and appropriate behavior on the Internet; mainly, e-mail. There are three motivational characteristics of being deviant on the Internet: obtaining software (material gain), revenge, and the challenge and fun in learning. All of these incorporate the different forms of deviance on the Internet. There are mainly two forms of Internet deviance I noticed: e-mail deviance and hacking.

"The most vulnerable to intrusion" - Electronic Mail

One of the main forms of deviance on the Internet is electronic mail. E-mail deviance is using e-mail and/or an e-mail account to commit Internet deviance. A common form of deviance is breaking rules of netiquette. One example, is forwarding mail without deleting the past addresses; therefore, people have to scroll down three to five pages before they even get to the message. This can be annoying especially if the someone's modem is slower than most. The three motivational characteristics of being deviant on the Internet can be seen with e-mail.

Sending Goods via E-mail

Although e-mail is generally not used to obtain pirated software there has been occasions of this. If the program is not that big and will not draw suspicion, it can be sent via e-mail. Many people are unwilling to do this because e-mail can be easily intercepted and traced if the sender is not careful. The receiver of the mail needs to save it to his/her e-mail account and then download the software program to their computer.

Another possibility of controlling this form of deviance is the Internet service provider (such as American Online, Compuserve, etc.) can limit the size of the e-mail; for example, a message greater than five megabytes will not be sent. Obviously, this policy will be difficult to implement because there are times when people need to send big files and e-mail may the most efficient form of communication.

For the most part, hackers will use e-mail as a communication tool to find out where the pirate sites are. A hacker must go through a system of steps in order to insure their anonymity. First, they must obtain an anonymous e-mail account somewhere (e.g. anon.penet.fi). An anonymous e-mail allows a person to send a message to another server, which is sent to another server, and so forth, although not full proof it is a safe method of eluding detection. Second, they must learn Pretty Good Privacy (PGP), an encryption software program for e-mail. The reason why PGP is so popular is that it ensures that an e-mail message will not be read by another person other than the receiver of the message. This is because the sender of the message sends a "key" to the receiver, which allows the receiver the only access to that message. Third, by encrypting their anonymous e-mail a hacker sends it to another hacker, who will return the message with a list of pirate sites. A hacker told me that an anonymous e-mail encrypted was virtually untraceable because the message would be sent to a server in Oregon, which then would be sent to another server and another server until it reaches its destination. But as another hacker pointed out, this is also "kinda scary" because if the system administrator is watching you, s/he will get suspicious if you keep sending encrypted messages that are sent anonymously. E-mail is the tool to which hackers use to obtain pirated software.

Revenge and Harassment

Most people will send harassing e-mail anonymously, in order, to protect their identity. The easiest way is to send a message through Netscape. One of the options in Netscape allows a person to send e-mail to other people. But the program does not verify who you are, in other words, the person can put false information in the who it was sent by and the e-mail address. In one instance, a student send an anonymous e-mail to his/her class' e-mail list stating that the professor is sick of school and that there will not be any more lectures for the rest of the semester...and that everybody will receive A's. Tracking where the message was sent would be easy because of the IP address stamped to every message. If the student was smart he would have sent it from a campus computer; thus, becoming unidentifiable. But he was not smart and sent it from home. He was caught and expelled from school. There are two main forms of revenge and harassment: physical and psychological.

Physical

Physical destruction is mainly done on a person's e-mail account and is the most damaging if a file is deleted because there are no ways to recover deleted files. For example, an advisor left his e-mail account logged in while he helped somebody with a computer problem. Meanwhile, somebody put a malicious command in his login file that deleted everything in his account when he logged in again. He tried to recover his files, but was unsuccessful.

Breaking In

Henry sent an e-mail message to President Clinton telling him that he sucks while using

Mark's account. Mark could not believe it and told Henry to send another message saying that the message was not sent by Mark but by Henry out of fear that the Secret Service was going to have a file on him.

Moreover, Tim showed me how easily it is to access another person's e-mail. Ironically, a third person broke into his e-mail account and was reading his mail. Tim, knew this because every time he opened up Pine (a program that lets a person read and write e-mail messages) the "new" message tag was missing on his new messages. Someone was accessing his messages and being a hacker felt the need to find out who and where the person was. He typed in some UNIX commands, but, was unsuccessful. He did change his password and kicked the person out of his e-mail account.

He then accessed his bosses e-mail messages using some UNIX commands. He confided that he usually did this during "evaluation" time and thought it would be interesting to read co-workers messages. He concluded that 99.9% of the messages were boring. (Wong, In Progress)

Modification of files

Another form of physical destruction is modification of files. Many advisors will leave their account logged on. For the most part other advisors will log them out and not do anything to them. I, on the other hand, will create files, such as "You_Are_Stupid" and warn them next time I am going to destroy your account. (This is only for advisors). People leaving their accounts logged in is quite frequent; and anyone, could view, modify, and destroy files on their accounts.

Finally, another type of modification is putting a logout command in the login file. A person will be in an infinite loop so that when s/he logs in it will the log the person out. The only way to fix this problem is to go to the System Administrator of his/her Internet service provider.

Psychological Harassment

From my experience anonymous e-mail allows a person to send mail without ever being detected. This is also has the potential to harass another person psychologically. For example, there is something called a Flash program, which flashes the screen making the computer inoperable until they reboot the machine. A person sends this to an unsuspecting user and when that person tries to access that e-mail the screen flashes and the computer becomes inoperable. The only way out is to reboot the machine and delete the e-mail message. One of the reasons why this message is untraceable is because the program allows you to type any fallacious information regarding who it is from and the e-mail address. The only thing that is traceable is the IP account (the computer's address). But tracing the person would be impossible if that person sends the flash message on campus.

Another example, is an advisor sent a friend of his an anonymous e-mail bomb. One of the options of sending anonymous e-mail (if a person uses an anonymous e-mail server) is how many messages can be sent to that person. He typed in 50,000. And the message flooded the system of the other user causing it to crash.

The Challenge and Fun in Learning

Trying to understand how to avoid detection when using anonymous e-mail is challenging. Part of the thrill is to see if you can avoid being caught and to get away with it. One of the ways is to learn how to use PGP. This program is not the easiest thing to understand and use. One advisor spent eight to ten hours trying to learn it. He had two machines next to each other, one with information on how to use it, and the other trying to use it.

The Electronic Postal Inspector

Mainly through laws and policies, social control of e-mail, attempts to regulate and deter illegal use of e-mail, e-mail accounts, and netiquette. Why does not the majority of people using e-mail send each other harassing messages? What prompts people to be careful about sending anonymous e-mail? Do people even care if they are caught? There are two main forms of social control that affects CU students: The Telecommunications Act of 1996 and CU's own e-mail policy.

"A bad piece of legislation" - The Telecommunications Act of 1996

In one section of the Telecommunications Act (CDA) there is a paragraph about harassment on the Internet. Obviously, any type of harassment, be in on the Internet or via postal mail is illegal. Although I do not think any laws will help control this type of deviance because of the ease of anonymous e-mail. Most advisors and people I have talked to say that this is impossible to enforce and Roger Ebert said “a bad piece of legislation.” Mainly, four-letter words will be censored, because children should not be exposed to this type of language or “lascivious” pictures.

“That Sucks” - CU’s own E-mail policy

CU is trying to stop e-mail deviance. This policy too has paragraphs and definitions of what type of activity is wrong. For example, anonymous e-mail is wrong and is punishable by the University. For the most part, advisors and people I have talked to say that this policy is wrong and impossible to enforce. Phillip Zimmerman said that it “sucked” and students “shouldn’t stand up for this.”

Strangely, an advisor sent a message to the Supervisor with the subject heading, “out of town.” Harmless enough, but, the Supervisor received an accompanying message by a System Administrator at CU warning that this could be a harassing e-mail message. CU’s policy does not allow System Administrators to read student’s e-mail messages without written permission first and it does not appear that the System Administrator in this case followed the policy (Wong, In Progress).

The last variable

But laws and policies do not make up all of the forms of social control. A lawyer sent out information on his attorney business via e-mail that if anybody needed any legal advice to talk to him. He sent this message en mass to a bunch of lists. Although I did not observe this at the lab the result was an uproar of people who flooded his system with e-mail in response that what he did was unethical. Moreover, Roger Ebert said that the best thing to do with people trying to advertise or sell products using mass e-mail is to ignore them.

Another netiquette that was broken is an Information Systems Organization (ISO) officer sent out an e-mail to BDM (a corporate sponsor of ISO) writing that he was displeased with the rude attention he received when he went in for an interview. There's nothing strange about a person being displeased with a company, but he sent his e-mail to the ISO e-mail list. The majority of the e-mail messages "flamed" (attacked the student) for being a "whiner" and that this is "part of life" and that he "should deal with it." The student who sent out the original e-mail sent another reply stating that he was sorry that this ever happened. BDM was not pleased with this incident. Nor were many students who wanted to disassociate themselves with that individual.

Hacking

There are many definitions of this and hacker. My definition is: a person who is knowledgeable about computers/systems/languages/Internet/etc. who is able to maneuver around systems and systems security so that s/he can learn more about them or can create better systems/systems security/and programs. There are different types of hackers. In my setting there were no reported "crackers," or people who deliberately destroy files, and programs for no apparent reason. An example of a cracker would be Kevin Mitnick. Mitnick was probably the most notorious computer criminal in the world because many financial analysts believed he stole billions of dollars worth of industry secrets. Moreover, he threatened to bring down a whole network (six thousand users) if he was ever caught by the authorities. The second type of hacker, is the Inquisitive one. This person wants to learn as much as s/he can by wandering the Internet. Learning is through experience, and the Inquisitive Hacker wants knowledge. S/he will spend hours trying to figure out problems, and making programs better. Finally, a third hacker, is the Materialistic one. This person wants software and other things s/he can obtain on the Internet. The Materialistic Hacker also encompasses the person who steals shareware versions of a program; as a result, is probably the largest group. All three can or already have commit the following deviant acts.

Superhighway Robbery

This is one of the rewards of being a hacker. As one hacker told me, " you get what you need." Most pirated software are available even before the product is released. Another hacker told me that he has boxes and boxes of diskettes of pirated software. This is one of the major reasons why people become hackers.

The only consequence to all of this is the time needed to download the software. Because most software now are pretty big it takes hours to just get one program. This is the reason why the lab is nice, especially at nights, because not many users are there and people can take up to five to ten computers. Moreover, CU's computers are able to "telnet directly to any site," making hacking much easier. One of the main reasons why one of the hackers became a hacker is because he wanted cool software. Moreover, he didn't want to spend a couple of hundred dollars on software that he could get for free.

The Internet has made software piracy much easier. All a person has to do is borrow a copy of a software program from a friend, surf the Internet for the correct patch program, which eliminates the copyright protection of a software's program. This has made it easier for people who pirate software to distribute it. These patch programs, and programs that can zip, and unzip files that are too big to put on a floppy disk are all easily available on the Internet. This is another way a person who does not have a lot of hacker knowledge to pirate software.

"It's the company's fault" - Shareware violations

This is a person who downloads an evaluation copy of a software that is only supposed to be used for a certain number of days and depends on using it past that deadline. For example, on the advisors machine there is a message that pops up when you start playing Duke Nuke'm 3D. "This game has been played 90 times! It is time to upgrade to the real copy now!!!" This is probably the most common form of Internet deviance at the computer lab. I think every male advisor has played that game, even though, "it is time to upgrade now." The consensus is that using shareware software past its deadline is something "you don't even think about."

Breaking and Entering

A hacker told me that he once broke into multiple accounts at another college. All he did was finger the person for personal information, saw that this person liked a band, and then he guessed his password; amazingly, he guessed right. He would then use those accounts to raid pirate sites. This was great for him because he would never get caught. In other words, he would go to a pirate site using the stolen account, from there he would download software to CU, and all the authorities could do was trace where the information was being sent to. But could never figure out who the person was.

Harassment and Revenge

Most of the destruction and modification of files is because of spite. The hackers would tell me that they did this because they thought the systems administrator was an "asshole" and he "deserved it." Similar to e-mail harassment and revenge there is physical and psychological forms.

Physical

The two hackers I spoke with were not generally destructive physically. One person actually said that being destructive was "sort of stupid" and that he had no desire to do things like that because he "wouldn't learn anything." But they both have done some damage if they didn't like the system administrator or just felt the need to do so. For example, one person got into a server in Germany and decided to destroy every configuration file in the system. Obviously, this caused a lot of damage and heartache to the system's administrator. The person felt like doing it, thought the system was an easy target, and was fun. All he did was sent a program to distract the security system of the server, while he walked through the "back door."

Modification of files

Again modification of files is another form of physical harassment and revenge. If one hacker didn't like a systems administrator he would modify files to annoy him/her. For example, a hacker would modify a systems Administrator's home page to read "I'm a fucking loser." Generally, when he did something like that he tried not to damage anything and if he did felt that it should only "take ten minutes to fix, if the system administrator knew what he was doing."

Challenge in Learning

Hacking was a hobby that was fun and took up a lot of time. They were able to get software they wanted and learn about the Internet/Systems/etc. They both stopped hacking because they didn't have the time anymore. "You get a full-time job and your hacking time decreases." "Also, because I have become a systems Administrator, the last thing I want to do is come home and stare at a computer screen." One person stopped because he lost "interest" and it wasn't "fun" anymore. Moreover, downloading pirated software took a long time. This is the reason why, I believe, most hackers pirate late in the night because there is less people on-line, therefore, download time was faster.

Learning was the main reason why one of the hackers started hacking. He wanted to learn everything possible about systems. The best way for him to do so was trying to break into them and probe around. There was no way that he would have become a systems administrator if he did not learn the things he did from hacking. Furthermore, he probably learned a lot about UNIX and other related things regarding the Internet.

One of the reasons why Mitnick was caught because he could not resist the challenge of going against Shimomura, "a computational physicist with a reputation as a brilliant cyber-sleuth in the tightly knit community of programmers and engineers who defend the country's computer networks." Mitnick broke into a computer owned by Shimomura, stole a lot of classified files (which he never used) so that he could entice Shimomura to find him. Mitnick even left taunting messages on the Shimomura's answer machine. This led to Mitnick's demise as Shimomura and the FBI was able to track him down. Mitnick and Shimomura finally met when he was caught. Mitnick responded to Shimomura, "Hello Tsutomu, I respect your skills."

Social Control

Unless a person is traced and caught, hackers are not deterred by intruding into systems or pirating software. They are obviously breaking laws and part of the challenge is not to get caught. The two main hackers quit because they wanted to and not because of somebody or something stopping or deterring them.

There are no forms of social control regarding obtaining shareware copies of a program, other than, the person feeling bad about having the evaluation copy that is a year past its deadline. Most people feel there is no way they can be caught. There are probably thousands of people hitting company sites for shareware software programs. As a result, there is no way the company could track all of those people. Moreover, at CU a person can go to a lab, download the software and remain anonymous to the company.

Another form of control would be to have the program die after a month or so of use. The easiest way around this is downloading the software again or keeping the original zip file stored somewhere so that it can be installed again after the program crashes.

One of the more interesting phenomena is that people do not feel that shareware violations are deviant, even though, they are breaking copyright laws. For the most part, I feel that this is because people do not feel that they can be caught. And in a way there is not any clear, easy way for companies to protect themselves from these copyright infractions. Lambchop felt that shareware violations was deviant, but, did not really care because it is the "company's fault for putting software out for people to take. Why should I pay for something that is free?"

Part of the reason why the hackers I observed felt invincible is because they do not commit the computer crimes that Kevin Mitnick committed. Mitnick was supposed to have a lot of information that would hurt a lot of companies. Most hackers are college students who pose little threat to a company's financial interest. But, if a hacker steps past the line of being a hacker and becomes a cracker, his/her status of a nuisance changes to a Mitnick; dangerous. Authorities, such as the FBI, obviously care about hackers and crackers but for the most part will not care about the hobby hacker.

Moreover, in order for the FBI to catch Mitnick they needed the help of a "computer sleuth" with the aid of high technological equipment, such as cellular scanners, to track Mitnick down. The FBI would not put the effort or equipment to track every college hacker who steals software who may cause occasional damage.

Conclusion

Although my main sources of information dealt with computer crime the language was relatively the same as that with Internet deviance. There is the "hacker" a person who is exceptional with computers and can maneuver around the computer and systems. There are similar goals, tactics, and motivations that revolve around computer crime. But there are differences, the Internet has allowed systems to be connected with one another in greater quantities then ever before. Therefore, allowing "hackers" to roam more freely. At one time, computer criminals had to be in the company as an employee for him/her to steal information from a computer; now, hackers can access a company's system with a phone line. This may be the underlying difference between computer deviance and Internet deviance.

The Chantico Publishing Company gave four motivational factors in becoming a computer criminal. The three are "resentment, a sense of gaming, challenge, and financial gain." Similar to my research, resentment, or revenge, makes hackers go. Their spite toward the system administrator, or another person brings on their wrath. One of the people I would not want to make mad is Kant. The next thing I know, I would be "officially dead," and my bank account wiped out.

A sense of gaming is another finding. This is also mentioned by Pfuhl. Like all hobbies, there is a need to invest time and resources, and is a learning experience. One of the inevitable results of being a hacker is the knowledge a person learns from it. For example, Tim was able to get his software, etc., but as a result, learned quite a bit about systems and UNIX. Similar to other research done, hacking is a game that is challenging and rewarding. The rewards are learning more about systems, and obtaining software that is beneficial to the hacker.

It is challenging because they have to ensure their anonymity or they will get caught. Also, outsmarting system administrators, who are supposed to know what they are doing, boosts confidence in oneself. Finally, hard-core hacking allows a person to be apart of an underground of people, mystical, intriguing, and most of all, fun.

Strangely, the Chantico Publishing Company decided to separate "challenge" and "sense of gaming." These two, and learning, are relatively similar and can be combined into one.

My third motivation for hackers is material gain. The fact that they can obtain software, worth hundreds of dollars, for free is one of the rewards and advantages of being a hacker. The Chantico Publishing Company mentions this as “financial gain” as a possible motivational reason why people become hackers. I do not feel that material and financial gain are the same. Material gain is obtaining software, while, financial gain, may encompass pirating software, but the main focus is obtaining money.

Hollinger’s ten acts of computer deviance can be applied to my research, but there are slight differences. “Acquiring another user’s password” and “Unauthorized use of someone else’s computer account” is relatively the same. Therefore they should be combined to make only one act.

Moreover, unauthorized storage of data would be one of the categories that would be pertinent to Internet deviance. One of the easiest ways of putting an illegal pirate site on the Internet is using a legitimate server to store the pirated software. For example, the Candyman home page discussed in the literature review.

Furthermore, Hollinger mentions that “deliberate damage or theft of computer hardware” is another act; which is impossible to a hacker connected by a telephone line. Lastly, hackers must break through “firewalls” or the computer system’s security against unauthorized entry. This is another form of deviance that probably was not well known because not many companies were on-line and needed the protection of firewalls. Other than these four, Hollinger gives an excellent overview of computer deviant acts that can be related to Internet deviance.

Hollinger briefly describes the different categories of computer criminals. They are the “pirates” or people who steal and receive illegal software programs. The “browsers” or people who “gain occasional access to another user’s university computer account” and finally the “cracker” or people who “copied, modified, and sabotaged other user’s computer files and programs.” For the most part, two of my hackers met all three of these definitions. This is probably the only downfall in these categories. There is no clear-cut line that distinguishes computer deviants.

Parker gives an interesting overview of hacker's actions to break into computer systems. For example, Tim told me how he got around a system's security system by using a program that distracted the computer while he sneaked through. According to Parker this would be labeled as the "Trojan Horse" approach.

Finally, one of the acts of deviance that is similar to my field notes is what the book calls "piggybacking terminals." Many people leave their e-mail accounts logged on; therefore, allowing people to view, edit, delete whatever files that are in their account. Referring back to an earlier example, an advisor left his account logged on and I created a file called "You_Are_Stupid." Although I did not do anything malicious I did violate another person's privacy and committed a form of deviance.

These are two of the many approaches Parker found that hackers commit. In my setting the "Trojan Horse" and "piggybacking terminals" are approaches that I came across; but, it does not mean that Parker is wrong considering my setting only deals with a handful of people. Expanding my research to encompass more people may prove Parker to be correct and maybe even find more ways hackers break into systems.

Moreover, he lists a category of crimes. They are sabotage, theft of services, property crimes, data crimes and financial crimes. All four are potential possibilities in committing computer crimes. But, in my setting, there were no financial crimes. Again, I do not believe that many hackers hack for financial gain. Even the most notorious hacker, Mitnick, did not care to use the information he had that was worth billions of dollars. Although I did not see it I have read that companies are now hiring crackers to sabotage their competitor's computers. This may be true, but not in my setting.

Bequai and Pfuhl noticed that there needs to be stricter laws in deterring hackers. As of right now, both believe the laws are inadequate. This stems from many people believing that hackers are not "true criminals," but, "good people" who are not "violent." For the most part, they argue that there needs to be some change because hackers can potentially hurt property and business. This can be evident with Kevin Mitnick who some systems analysts believed had billions of dollars worth of trade and corporate secrets; not including, the twenty-thousand credit card numbers that he obtained by breaking into a credit card company's files. Although I know that there are hackers out there who want to gain financially, from my research and reading about Kevin Mitnick, hackers do not want to gain financially (except maybe software) but is the challenge and fun of eluding authorities.

> Indeed, frequently ignoring the possibility of straightforward financial gain from the information he has stolen. Mitnick has often seemed more concerned with proving that his technical skills are better than those whose job it is to protect the computer networks he has attacked. (NY Times)

This is also similar to Kant, who boasted that "I can't believe how stupid sys. admins. are when they have a two hundred megabyte pirate site on their system." Moreover, for Kant, there was a need to prove himself, "I didn't do anything that a sys. admin. couldn't figure out in ten minutes. And if he couldn't he's stupid and shouldn't be in that job."

Marx's theory that Internet deviance is easy because it is hard to relate a human person on the other end can be found with the hackers I interviewed. For instance, Mark sent an anonymous e-mail to the Information Systems Organization's (a student club) president, "Fifty Reasons why Bitches should not talk." She was not happy. Many deviant cases I encountered involved people not caring about the damage done to another person because s/he was "invisible."

Because the lab is closed at midnight, this an opportune time for many hackers, partly because downloading software will be faster because of less users on-line. I hypothesize that because Engineering remains open all night and has no supervision (because the advisor office closes at midnight) the potential for Internet deviance, especially hacking, increases.

Although all my hackers are white male it does not mean there are no female or minority hackers. This is just a result of research at a computer lab that does not have many minority advisors. Another hypothesis, however, is that hacking is generally dominated by white males. Partly, because engineering students are males and that on the whole whites have greater access to resources regarding computers and computer knowledge (e.g. computer classes in high school).

A final hypothesis would be that software programs will decrease in price as more people obtain pirated software copies. This is due to the easy access of the Internet and the tools available on-line that make pirating easier (i.e. zip programs that shrink the size of a file to its bare minimum). Although hacking will not disappear, as long as there is a system to invade, there will be a shift in motivations as one of the rewards of hacking (getting free software) will disappear. Maybe the next goal of hacking is to steal money from companies. Or hackers will be hired corporate spies that sabotage a competitor's important files.

Nevertheless, hacking will remain, regardless of the social control to deter and punish hackers. The three motivations will always be there: material gain, knowledge, and the challenge and fun in hacking. As systems become more complex, the hacker will always want to crack it out of conquest and knowledge. The knowledge s/he gains from hacking is invaluable for him/her if that person wants to pursue a career in a computer related field. Moreover, the challenge of cracking a system is irresistible for many hackers. This is the fun and the excitement. And the main reason why many people spend countless hours in front of a computer terminal.

Bibliography

Bequai, August. 1978. *Computer Crime*. D.C.: Lexington Books.

Bequai, August. 1978. *White Collar Crime*: A 20th Century Crisis. D.C.: Lexington Books.

Chantico Publishing Company, Inc. 1992. *Combating Computer Crime*. NY: McGraw Hill, Inc.

Conference on World Affairs. 1996. Open and Closed: Bullies, Hackers and Saints - The Internet Changes it All. April 12. Roger Ebert, Burgess Laird, Oliver McBryan, Ulrich Trottenberg, and Phillip Zimmerman were the panelists.

Correll, Shelley. 1995. The Ethnography of an Electronic Bar. *Journal of Contemporary Ethnography*, Vol. 24 No.3, October, 270-298.

CU's own E-Mail Policy. 1996. http://www.colorado.edu/HyperHelp/news-info/email.html

CU's own Appropriate Computer Behavior Policy. 1996

Henry, Stuart and Pfuhl, Erdwin H. 1993. *The Deviance Process*. NY: Aldine De Gruyter.

Hollinger, Richard C. 1988. Computer Hackers follow a Guttman-like Progression. *Sociology and Social Research*, Vol. 72 No. 3, April, 199-200.

Hollinger, Richard. 1993. Crime by Computer: Correlates of Software piracy and Unauthorized Account Access. Security Journal; 1993, 4, 1, Jan., 2-12.

Katz, Jack. 1988. *Seductions of Crime*. NY: Basic Books, Inc., Publishers

Markoff, John. 1995. A Most-Wanted Cyberthief is Caught in his own Web. *New York Times*, February 16.

-------. 1995. How a Computer Sleuth Traced a Digital Trail. *New York Times*, February 16.

-------. 1995. Hacker case Underscores Internet's Vulnerability. *New York Times*, February 17.

Marx, Gary. 1994. New Telecommunications technologies require new manners. *Telecommunications Policy* 18: 538-551.

Marx, Gary. 1991. The New Surveillance. National Forum; 1991, 71, 3, Summer, 32-36.

Marx, Gary. 1988. *Undercover*. Berkeley: University of California Press.

Marx, Gary. 1988. Privacy and Technology. Many articles

Mendels, Pamela. 1996. On-Line Newspaper's Provocation to Test Decency Act. *New York Times*, April 26.

Parker, Donn. 1976. *Crime by Computer*. NY: Charles Scribner's and Sons.

Pfuhl, Erdwin H. 1987. Computer Abuse: Problems of Instrumental Control. *Deviant Behavior*, 8:113-130.

Shimora, Tsutomu. 1996. Takedown: Pursuit and Capture of Kevin Mitnick. NY: Hyperion.

Whiteside, Thomas. 1978. Computer Capers. NY: Thomas Y. Crowell, Publishers.

Wong, John. In Progress. Caught in the Web: Social Control of Electronic Mail.