Computer crime 3403 essay

It’s the weekend, you have nothing to do so you decide to play around on your

computer. You turn it on and then start up, you start calling people with your

modem, connecting to another world, with people just like you at a button press

away. This is all fine but what happens when you start getting into other

peoples computer files. Then it becomes a crime, but what is a computer crime

really, obviously it involves the use of a computer but what are these crimes.

Well they are: Hacking, Phreaking, & Software Piracy. To begin I will start

with Hacking, what is hacking. Hacking is basically using your computer to

“ Hack” your way into another. They use programs called scanners which

randomly dials numbers any generating tones or carriers are recorded. These

numbers are looked at by hackers and then used again, when the hacker calls up

the number and gets on he’s presented with a logon prompt, this is where the

hacking really begins, the hacker tries to bypass this anyway he knows how to

and tries to gain access to the system. Why do they do it, well lets go to a book and see “ Avid young computer hackers in their preteens and teens are frequently involved in computer crimes that take the form of trespassing, invasion of privacy, or vandalism. Quite often they are mearly out for a fun and

games evening, and they get entangled in the illegal use of their machines without realizing the full import of what they are doing”, I have a hard time believing that so lets see what a “ hacker” has to say about what he does “ Just as they were enthraled with their pursuit of information, so are we. The thrill of the hack is not in breaking the law, it’s in the pursuit and capture of knowledge.”, as you can see the “ hacker” doesn’t go out to do destroy things although some do. It’s in the pursuit of knowledge.

Of course this is still against the law. But where did all of this start, MIT is where hacking started the people there would learn and explore computer systems

all around the world. In the views of professional hacking is like drugs or any other addictive substance, it’s an addiction for the mind and once started it’s

difficult to stop. This could be true, as hackers know what they are doing is wrong and they know odds are they will be caught. But as I mentioned some hackers are just above average criminals, using there skills to break in banks and other places where they can get money, or where they can destroy information. What a hacker does at a bank is take a few cents or even a few fractions of a cents from many different accounts this may seem like nothing but when all compiled can be alot. A stick up robber averages about $8, 000 each " job", and he has to put his life and personal freedom on the line to do it while the computer hacker in the comfort of his own living room averages $500, 000 a " job". As for people destroying information, this is for taking some one down, destruction of data could end a business which for some is very attractive. It can cost a company thousands of dollars to restore the damage done. Now that you have an understanding of what a " hacker" is, it time to move on to someone closely associates with a hacker. This is a Phreak,

but what is that. For the answer we turn to the what is known as the

“ Official” Phreakers Manual “ Phreak [fr’eek] 1. The action of

using mischievous and mostly illegal ways in order to not pay for some sort of

telecommunications bill, order, transfer, or other service. It often involves

usage of highly illegal boxes and machines in order to defeat the security that

is set up to avoid this sort of happening. [fr’eaking] v. 2. A person who uses

the above methods of destruction and chaos in order to make a better life for

all. A true phreaker will not go against his fellows or narc on people who have

ragged on him or do anything termed to be dishonourable to phreaks. [fr’eek] n.

3. A certain code or dialup useful in the action of being a phreak. (Example:

“ I hacked a new metro phreak last night.”)” The latter 2 ideas of

what a phreak is, is rather weird. A Phreak like the hacker likes to explore and

experiment, however his choice of exploring is not other computer but the phone

system as a whole. Phreaks explore the phone system finding many different ways

to do things, most often make free calls. Why do they do this, ” A hacker

and phreaker will have need to use telephone systems much more than an average

individual, therefore, methods which can be used to avoid toll charges are in

order. “. A phreak has two basic ways of making free calls, he can call up

codes or PBXs on his phone and then enter a code and make his call or he can use

Electronic Toll Fraud Devices. Codes are rather easy to get the phreak will scan

for them, but unlike a hacker will only save the tone(s) number instead of the

carrier(s). Then he will attempt to hack the code to use it, these codes range

from numbers 0 – 9 and can be any length, although most are not more than 10.

Electronic Toll Fraud Devices are known as Boxes in the underground. Most are

the size of a pack of smokes, or than can be smaller or bigger. I will not go

too deep. They are electronic devices than do various things, such as make

outgoing calls free, make incoming calls free, simulate coins dropping in a

phone, etc. People who “ Phreak” are caught alot these days thanks to

the new technology. Software Piracy is the most common computer crime, it is the

illegal coping of software. “ People wouldn’t think of shoplifting software

from a retail store, but don’t think twice about going home and making several

illegal copies of the same software.” and this is true because I myself am

guilty of this. The major problem is not people going out and buying the

software then making copies for everyone, it’s the Bulletin Boards that cater to

pirating software, that really cause the problem. On anyone one of these boards

one can find an upwards of 300 – 1000+ of pirated software open for anyone to

take. This is a problem and nothing can really be done about it. Few arrests are

made in this area of computer crime. I will now devote a brief section to the

above mentioned BBS’ , most are legal and do nothing wrong. However there are

many more that do accept pirated software, pornographic pictures, animations ,

and texts. As well as a trading area for phone codes, other BBS', Credit Card

numbers, etc. This is where a majority of Hackers and Phreaks come, as well as

those who continue to pirate software come to meet and share stories. In this is

a new world, where you can do anything, there are groups that get, crack, and

courier software all over the world some of them are called: INC: International

Network Of Crackers, THG: The Humble Guys, TDT: The Dream Team. As well a number

of other groups have followed suit such as Phalcon/SKISM (Smart Kids Into Sick

Methods), NuKE, and YAM (Youngsters Against McAfee) these are virus groups who

write and courier their work anywhere they can, they just send it somewhere,

where anyone can take it and use it in any manner they wish, such as getting

even with someone. All of these activities are illegal but nothing can be done,

the people running these boards know what they are doing. As it stands right

now, the BBS world is in two parts Pirating and the Underground, which consists

of Hackers/Phreaks/Anarchists/Carders(Credit Card Fraud)/Virus programmers. All

have different boards and offer a variety of information on virtually any

subject. Well from all of this reading you just did you should have a fairly

good idea of what computer crime is. I didn’t mention it in the sections but the

police, phone companies are arresting and stopping alot of things every day.

With the new technology today it is easier to catch these criminals then it was

before. With the exception of the BBS’ the police have made some major blows

busting a few BBS’, arresting hackers and phreaks. All of which were very looked

up to for knowledge in their areas of specialty. If I had more time I could go

into these arrests but I must finish by saying that these are real crimes and

the sentences are getting harsher, with alot of the older people getting out the

newer people are getting arrested and being made examples of. This will deter

alot of would-be computer criminal away. The word virus can be very

disheartening, especially when computers are involved. A virus is composed of

instructions hidden inside a program. These instructions copy themselves to

other programs, and the cycle continues spreading. Fortunately, help is

available; antivirus software is available to anyone. “ Viruses first

appeared in 1985. Then, they were largely created in university laboratories by

mostly wayward geniuses keen to pit their programming skills against each other.

Since then, errant programmers began to create newer and more destructive

viruses targeted at specific user groups.” (Yang, 1998) A computer virus

can be as “ evil as it sounds, snaking its way into personal computers,

posing an occasional annoyance or a serious threat to all data.” (Miastkowski,

1998) Symptoms can range from unpleasant to fatal. Computer viruses spread from

program to program and computer to computer, “ much as biological viruses

spread within individual…members of a society.” (Chess, 1997) Diskettes

were the “ primary carriers of viruses in the 1980s.”

(“ Computer,” 1997) Today, they are e-mail attachments, file transfers

and infected software downloads or uploads. Networks can even spread viruses to

large numbers of connected PCs rapidly. (Yang, 1998) No one working on a

[personal computer] is risk free; more viruses are being spread today than ever

before, but more help is being developed as well. Special software is now in

stores that will help to prevent any major disasters that viruses can cause. (Miastkowski,

1998) Antivirus software is a program that protects against viruses. It scans

all files on the hard disk, diskettes, CD ROM, and memory to locate viruses.

(“ Computer,” 1997) The life cycle of a virus is rather complicated; it

begins when a user runs an infected program. The computer copies the program

from the disk into RAM, random access memory, where it can be performed. The

viral code begins to run, and the virus copies itself into a part of RAM that is separate from the program. This allows the pesky virus to continue to spread while another program is running, until it is finished and passes back into the infected program. “ When the user runs a different program, the dormant virus begins to run again. It inserts a copy…into the…uninfected software so that the cycle…can repeat.” (Chess, 1997) There are also other computer pests such as “ worms” that effect networks, but viruses are the most common. (Yang, 1998) Years of research have allowed scientists to find ways to

detect and destroy viruses. (Chess, 1997) “ Building on decades of research by mathematical epidemiologists, [researchers] have obtained some understanding

of the factors that govern how quickly viruses spread.” (Yegulalp, 1997) Many researchers feel that they owe much to “ pattern-matching techniques developed by computational biologists.” (Chess, 1997) This has helped them to develop antivirus software from the defenses used by the human body to fight

off pathogens. According to an independent survey by the National Computer

Security Association, the infection rate for personal computers in North America

has more than tripled in the last year. (McDonald, 1997) “ In the 1990s, the

virus problem has become an epidemic. New forms, including the shape-changing

polymorphic virus, elusive stealth strains, and the very common macro viruses

are making their appearance with alarming frequency.” (Yang, 1998) The

macro viruses are big problems; they infect very popular programs such as

Microsoft Word and Microsoft Excel. This type of virus can effect daily work

much easier than any other virus. (Miastkowski, 1998) “ Almost any [antivirus]

package does a nice job of finding and eradicating most viruses, including macro

viruses. The key is to keep the products’ library of signatures–binary code

that helps identify viruses–current.” (Yegulalp, 1997) That is one area

where these packages differ most. Some of the major brands of antivirus software

include Norton AntiVirus 4. 0, PC-cillin 3. 0, Dr. Solomon’s Anti-Virus 7. 0, McAfee VirusScan 3. 0, and IBM AntiVirus 3. 0. 1. (Miastkowski, 1998) “ All the programs share some common attributes; for starters…each program indeed hunts down and eradicates the bugs introduced into a system.” (Cope, 1998) By far, the best at detecting and destroying viruses is Norton AntiVirus 4. 0; it offers superior protection. This particular software uses a virus-detection technology called “ Bloodhound.” It “ sniffs out viruses that may have been mutated beyond their original forms.” (Yegulalp, 1997) TouchStone’s PC-cillin 3. 0 follows closely behind Norton AntiVirus 4. 0; it provides sufficient protection, and updates are available over the internet. (Miastkowski, 1998) “ Each program scans or boot-sector and memory-resident viruses automatically when [the user] turns on the computer.” They also include a Windows 95 antivirus shield that blocks contamination from infected floppy disks and warns the user when a tainted file is being run. “ In addition, they let users perform manual scans of any drive from within Windows 95, and also

check…files downloaded from the Internet.” (Cope, 1998) “ Norton AntiVirus 4. 0 generously incorporates its Windows NT, DOS, Windows 3. x and Windows 95 editions into one package. PC-cillin also runs under NT, although TouchStone ships the NT edition as a separate product.” (Yegulalp, 1997)

Another advantage to the Norton AntiVirus software is the installation process; it is not difficult, and several options are provided for the user. Norton AntiVirus can load live protection and allow the user to create a rescue disk set. The rescue disk set backs up the system, allowing the user to boot and recover from a virus attack. (“ Hackers,” 1997) The PC-cillin software is very protective also. “ Upon installation, PC-cillin immediately makes sure its own files are clean, since an infected antivirus program is powerless to prevent further infection.” (Yegulalp, 1997) This program also offers a backup system and scan of the system before Windows 95 loads. (Yang, 1998) The latest version of PC-cillin informs the user as it is scanning an internet connection. It “ offers much tighter functionality than before. Earlier PC-cillin

users will definitely want to upgrade.” (Yegulalp, 1997) On the surface, it looks as if the odds are against personal computer users. Despite increased use of antivirus software, viruses continue to spread at an unnerving rate. (McDonald, 1997) Clearly, anti-virus software is one of the smartest buys a computer owner can make. There are nearly 10, 000 known computer viruses threatening the world’s personal computers, “ with effects ranging from relatively harmless to ferociously destructive.” (Cope, 1998) These troublemakers can spread to personal computers easily from an infected floppy disk, as well as from files downloaded onto the hard drive from an e- mail attachment and the Internet. (McDonald, 1997) Despite the great reviews of these antivirus programs, many computer researchers maintain a sense of skepticism towards complete protection. “ Regardless of how sophisticated antivirus technology may become, computer viruses will forever remain in an uneasy coexistence with us and our computers.” (Chess, 1997) Unless there are

updates to virus scanners every few minutes, no one is completely safe from a

destructive virus. New viruses are popping up so fast that virus scanner vendors

cannot hope to keep up with them. Even with the best of tools and policies,

“ bulletproof security is probably unattainable. High costs, changing

networks and software versions, incomplete security tools, and the growing pool

of ingenious and dedicated hackers prohibit this.” (“ Hackers,”

1997) The numbers of people who can create new viruses have also increased.

(Yang, 1998) “[In June 1997], a group of hackers quickly cracked a

much-vaunted…code using relatively simple brute force techniques.”

(“ Hackers,” 1997) This breach of security was only five weeks after

the data security invited the attack in the hope of proving its codes resistant

to such attacks. Over several years, people have been perfecting the care of

personal computers. However, over that same amount of time, others have been

hard at work to develop new ways to cause a system to “ crash.” Some

problems with a personal computer cannot be stopped, but preventative action can

take place for viruses. Every computer user should be equipped with an antivirus

program; there is no way of predicting whether or not a simple file contains a

tremendous virus. The user must leave such a decision to the computer itself;

only it can detect and destroy the virus. By purchasing a simple antivirus

package, each computer user can hamper viruses from entering and destroying his

personal computer. After taking all of the costs into consideration, it is much

more expensive to rebuild a computer after destruction than it is to purchase an

effective antivirus software package.

Bibliography

Chess, David, Jeffrey Kephart, Gregory Sorkin, and Steve White.

“ Fighting Computer Viruses: Biological Metaphors Offer Insight into Many

Aspects of Computer Viruses and Can Inspire Defenses Against Them.”

Scientific American Nov. 1997: 134-138. “ Computer.” The World Book

Encyclopedia. 1997. Cope, Jim. “ A Buyer’s Guide To Virus Protection: Get the Lowdown on Six Win 95 Programs that Keep Digital Bugs from Invading your PC and Destroying your Files.” NetGuide Mar. 1998: 143-146 “ Hackers, Terrorists, and Spies: You know they’re coming at you. Can you stop them?” Software Magazine Oct. 1997: 76. McDonald, Glenn. “ Viruses: An Anatomy of Mass Hysteria.” PCWorld Sept. 1997: 123-125 Miastkowski, Stan. “ Virus Killers 1998: This Year, Macro Viruses are Running Rampant. Which Antivirus Program is Your Best Defense?” PC World Mar. 1998: 114-116. Yang, W. D. “ Be Aware of Viruses and Use Protection.” Computer Times 18 February 1998: 85-89. Yegulalp, Serdar. “ Head to Head: Antivirus Software Virus Protection Superheroes.” Windows Magazin