Computer hacking is ethical essay

Computer Hacking is Ethical Computer hacking is a term that most everyone in today’s society is familiar with. When the average person hears news about computer hacking, most likely they think about cyber-crimes, website defacement’s, or knocking various websites offline. This inaccurate description is Just the image that today’s media creates. In reality, true hackers are much different. Computer hacking is not the only type of hacking in today’s society.

Hacking actually originated from appearing, which is the art of racking a telephone network (“ A Brief History of Computer Hacking”). Hacking is seen as being blackout, or wrong, when hacking can also be beneficial to the world. There are different types of computer hackers: “ Hastiest,” ones who hack to express a political opinion, “ Hobbyist” hackers, those who hack for enjoyment, and “ Research hackers,” those who hack to learn about security and fix vulnerabilities (“ License to hack? Ethical hacking”). As mentioned before, the first computer hackers were not people who were hacking to earn some quick cash. In 1878, two years after the telephone was invented y Alexander Graham Bell, a group of teenagers who worked to maintain the New York switchboard were fired because they were interested in seeing how the phone connections were made and how the calls were distributed to specific locations. Their actions were essentially the equivalent of early computer hackers.

These boys were trying to break into the telephone system to understand and see how the switchboard worked (“ Timeline: A 40-Year History of Hacking”). Computers were not always in the easy to use, graphical interface they are today. Along the time period of the ass, mainframe computers were very popular. Most universities and companies would have rooms dedicated to containing these mainframes computers, which were essentially a large chunk of metal locked away in a controlled environment. Due to the prices and exclusivity, users had to fight for time to obtain access to these slow-moving machines.

Since these mainframe computers were so expensive and resource intensive, meaning they required time, knowledge, electricity, and money, computer programmers went out on a ledge to learn and create ways to speed up processes and modify hardware to increase performance speed (“ Computer hacking: Where did it begin and how did it grow?). In return, the machine would be able to complete more tasks and operations in a shorter time period. Hiring a hacker to modify one’s machine in the ass and ass would definitely increase business functionality (Parks).

The term “ Hacker” did not earn the definition it has in today’s world until the sass. Users discovered that they could apply their knowledge of the inner workings of a computer for their own gain. This was the time period when viruses, mallard, and other nasty cyber infections were created to earn their coder or hacker money (“ Timeline: A 40-Year History of Hacking”). In the early sass, a man named John Draper discovered that he could recreate the pitch a telephone used by using a whistle obtained from a box of cereal.

By using this whistle, Draper could recreate the 2600-hertz audio tone and score some free long-distance calls. Draper’s actions were one of the first illegal actions committed by a hacker, which earned him the nickname “ Captain Crunch. ” Later in the sass, devices called “ Blue Boxes” were invented by a computer club in California. These boxes were used to help change a tone to match the tone created by a telephone, thus making telephone tampering easier to use. These boys went by the names of Steve Jobs and Steve Woozier, the creators of Apple Inc. " Timeline: A 40-Year History of Hacking"). Attention towards appearing was created during this decade, resulting in a few computer and telephone hacking magazines being created. These magazines would benefit those who wanted to become preparers and computer hackers, by teaching them techniques, and giving access to those who had already accomplished these illegal acts (" Timeline: A 40-Year History of Hacking"). Another effect from the huge amounts of attention towards hackers was a new law being passed, called The Comprehensive

Crime Control Act, giving the Secret Service Jurisdiction over cases including credit card and computer fraud (" INCURS Abstract"). Later in 1987, a seventeen-year-old hacks into AT's computer network, which led to his arrest. This boy was caught because he did want most teenage boys do, he bragged on an online bulletin board about it. Federal authority says he committed the hacking from his bedroom, and was one step away from breaching into AT&T's switching system, the system that controlled most of the nation's communication access fine (" Timeline: A 40-Year History of Hacking").

In the year 1988 the first self-replicating virus was created by a twenty-two year old graduate named Robert Morris from Cornell University that was designed to take advantage of an exploit in UNIX-based systems. The Morris-worm, named after the creator, infected nearly one tenth of machines connected to the internet. Morris was arrested for releasing the virus and was sentenced to three years of probation, 400 hours of community service, and a $10, 000 fine (“ Zen and the Art of the Internet”).

No other major hacks occurred until the mid to late ass, when two hackers known as Data Stream hacked into computers and systems owned by institutions such as NASA and Korean Atomic Research Institute. One of the two was caught by detectives form Scotland Yard and was discovered to be sixteen years old (“ The Case Study: Rome Laboratory, Griffins Air Force Base, and NY Intrusion”). The year after, Vladimir Levin allegedly used his laptop to transfer funds from Citibank’s computer network to various accounts across the world. Eventually Levin was extradited to the US, sentenced to three years in prison, and ordered to pay Citibank $240, 000.

The exact amount of money stolen is unknown, but is estimated to be around $3. -$10 million, not all of which has been recovered (“ How To Hack A Bank”). Later that year legendary computer hacker Kevin Nitpick was arrested in Raleigh, North Carolina, and accused of breaking security violations, such as copying computer software, breaking into various networks and stealing information, including close to 20, 000 credit cards. He spent four years in Jail without trial and was released in early 2000. Nitpick was accused of crimes dating back to the mid-sass (“ Timeline: A 40-year history of hacking”).

After the year 2000, many to most cyber- attacks or hacks have been caused by mallard users unknowingly downloading them onto their PC. Most newly created enamelware bypasses anti-virus scans, which means no one is ever one hundred percent safe on the internet. The graph below displays the type of virus or mallard threats received on various US computers (“ Microsoft Security Intelligence Report”). Every computer hacker is powered by a motive or several motives. Usually malicious hackers are motivated from self-gain, either money or fame.

Malicious programmers create mallard programs to do their bidding; such software can log every key one presses, steal sensitive data such as passwords for personal and banking websites, r add one’s computer to a ring of infected computers that can be used to Dodos websites (“ Ethics in Computing”). A Dodos attack is when packets of data are sent to a Webster that eventually overload the server with data to the point where the server crashes, therefore knocking the website offline. More recently, Anonymous has taken credit for Dogging major banking websites offline (“ Bank of America Hit By Anonymous Dodos Attack”).

There are many different types of Dodos attacks; the most common is a JODI Flood, which sends a JODI packet to random ports on a server. When a packet is sent to a port where there is no application listening on that port, the server replies with a Destination Unreachable packet, so the server has to respond to every single JODI Packet with an Unreachable; the part that crashes the server is when the Unreachable Packet is sent (“ UDP Flood Attack”). Hackers sometimes will sell their bootee, which is the term that describes a ring of infected computers.

When a hacker sells or rents his bootee, the infected PC’s are transferred over to the buyer for their use, which is usually for more illegal Dodos attacks. There is extremely easy money when it comes to selling information attained from hacking, whether it is selling hacked website accounts for popular websites like Youth or websites that require a monthly subscription. Most of the transactions are made online and are close to untraceable. Finding a competent hacker on the internet is the equivalent of going to Iraq and looking for AY Quad.

Hackers know how to hide, where to hide, and how to stay safe (“ Hackers Selling Cheap BOOTEES and DODOS on Forums”). Even though hackers know how to hide, that does not mean they cannot get caught. Hacker Jon Paul Soon illegally hacked into his previous employer’s network with malicious intent. This network was a medical network that contained health records, names, addresses, and provided services to seventeen different clinics in San Diego. Soon was punished with five years in prison and a combined fine of over four hundred thousand dollars, along with a ban from using a computer (“ Hackers: Crimes and punishments”).

Teenage hackers usually get off easier, with punishments like time in a Juvenile center, a ban from computers, community service, or very light prison sentences depending on age. FBI informant Max Butler was a hacker who was charged in 2001 with possession of stolen passwords, computer intrusion, and thirteen other counts. He risked going to prison for forty years because he decided to stop helping the FBI catch other hackers. These are Just a few cases of the risks hackers take for the thrill or self-gain from hacking (“ 5 Of the World’s Most Famous Hackers ; What Happened to Them”).

With such strong consequences, one might wonder why an individual would want to become a computer hacker. Internet users become hackers because they know how to work the system; they know how to yap's the law and do close to anything they want (" The Hacker Work Ethic"). Hackers are purely cyber thieves who terrorize innocent users using their superior knowledge of how computers and the internet work. There are indeed an abundance of hackers who have malicious intent, but there are those who hack for a higher purpose (Roberts).

Identifying what type of hacker one is dealing with is extremely easy; all one must do is look at the end product and ask a few questions. Is this hacker trying to steal information? Is the hacker trying to infect systems? If so, then that hacker is malicious. Other hackers hack for the learning experience. They want to learn more about computers and how systems change when modifying specifications. Hacker Sarah Flannels describes the work she put into her encryption algorithm as, " I had a great feeling of excitement … Worked constantly for whole days on end, and it was exhilarating.

There were times when I never wanted to stop. " Pursuing knowledge has been the fuel for many computer users since the first computers were created in the sass. These people live by the idea that the best way to learn is to take a hands on approach (" Types of computer hackers"). Contrary to black hat hackers, a type of hacker exists known as the white hat hacker. White hat hackers are the people who help infected users on the web. Many black hat hackers such as Kevin Nitpick, Kevin Paulsen, and Mark Been have turned white hat after serving time in prison or on probation (" 12 " White Hat" hackers you should know').

Not only to white hat hackers try to reverse the effects of black hats, but they also hack websites. Many businesses hire penetration testers, A. K. A. White hat hackers to try to penetrate the businesses' servers or databases to test how protected the businesses' websites are. Penetration testers, commonly referred to as Pen Testers, report back any exploits they have covered while hacking their employer's website or database, and then they patch the exploit, thus making a safer internet.

Companies believe that if a white hat hacker can penetrate their security, then so can a mischievous black hat hacker (" tithe hat' hackers in demand"). An example of a famous white hat hacker is computer analyst and expert Touts Shimmer, who police used to track down and apprehend Kevin Nitpick in 1995 after Nitpick had evaded the FBI for years, and caused well over $100, 000 in damage to systems belonging to Motorola, Monika, Sun Microsystems, and NECK (" The trials of Kevin Mitotic <).

This is Just one example of a hacker being caught by another hacker. Police computer security analysts and hackers to look decipher cyber evidence that is related to crimes under investigation, along with cyber-forensics to break down crimes and solve them quickly (" The Kevin Nitpick/ Touts Shimmer affair"). Hollywood has also tried to portray computer hacking in movies such as Hackers, from 1995, and War Games from 1983.

The movie Hackers is about two computer hackers named Crash Override and Acid Burn, who seemingly fight each other with silly fonts and awful homepage graphics. Later on in the movie, he US Secret Service is involved when another associate of Overrides hacks into a school's mainframe and downloads a garbage file. This file actually contained a computer virus that could apparently capsize the company’s oil tanker fleet. After a few other friends are arrested, everyone is cleared of their charges and the movie ends happily.

In reality, all of these hackers would have been in prison, and would not had their charges dropped, not to mention the fact that a company had the code to a computer virus that could control their entire oil tanker fleet on a garbage file in their easily hackle mainframe (“ Hackers”). Legitimate hackers later defaced the movie Hacker’s website to express how they felt about the silliness in this movie (“ Hacked Movie Site”). Nothing really big happened, only some text was changed and a few pictures were defaced with satirical pictures drawn over them.

The website still has the hacked version of their website mirrored, meaning it is still accessible to the web. Included in the text of the defaced website were lines describing how Hollywood misunderstands technology and will never be able to comprehend the hard work and time needed to perform some of the acts that hackers accomplish. No en can tap a few keys on a keyboard and hack into a company’s mainframe, website, or database.

Hackers included a scene where someone managed to access a supercomputer with Just the password “ GOD” and has the UNIX operating system replaced with some other three dimensional interface does not represent the real world in any manner (“ Episode – Hackers”). The movie Live Free or Die Hard also butchers computer hacking in the sense that the computer hacks in it are so good at hacking that they can control entire cities, including quotes like “ Okay, I want you to hack into that traffic light and make it red.

Almost all of the incredible feats provided by Hollywood in movies is practically impossible, or would require months of research to perform. Many hackers believe that Hollywood will never portray legitimate hackers correctly (“ Hollywood Hacking – Television Tropes & Idioms”). Computer fanatics are compelled by the mystery of the machine. When Mr.. Hake, the Computer Applications teacher from Erwin High was asked why he was so fascinated by computers when he first had access to them, he replied with, “ They were new and exciting; no one really knew where we were going to go with amputees, but everyone seemed to want to use them. ” Mr..

Hake described that people were compelled to study computers due to their mysteriousness and interesting possibilities (Hake). Switching from being a computer fanatic to being a computer hacker can happen really quickly when one may see how easy earning, or stealing money actually is on the internet. Or maybe the thrill of breaking past security will push the moderately to advanced computer user to turn to the dark side of computer hacking. Malicious hackers will always have a hard time as long as the be is full of white hat hackers to make their Job, or hobby more difficult (“ Meaning of Hacking and the Different Kinds of Hackers”).

In conclusion, not every person who knows their way around a computer’s boundaries is unethical. While there are many intelligent and malevolent hackers loose on the web, it is still a safe place. Today’s media does not accurately portray hackers or the hacker’s philosophy, and neither do cutrate Hollywood movies. Media websites control how civilians see cyber criminals, due to that factor, most innocents see hackers has people who are out to no good. The white knights of the internet are never given the appreciation they deserve, because of them we are as safe as we are now.

White hat hackers have patched countless exploits caused by bad-natured hackers. Governments can Jail as many hackers as they want, but they can never Jail a philosophy. Hackers will always exist; they will always be out to gain something out of their exploits. Society needs to understand that hackers also hack to prevent collateral damage, or to catch the worst of the worst hackers. There are good hackers and bad hackers, Just as there are good people and bad people; not all hackers are unethical.