

Computer crime essay sample



**ASSIGN
BUSTER**

Computer Crime had been defined broadly, though most text books agree that it is a criminal act that has been committed using computer as the principal tool. The types of crime which are regard as a computer crime can also vary depending on the text book you read. Nevertheless almost all of them have the same view, that hacking is one types of a computer crime. In this essay I will examine how hackers defend their action, argument and justification as well as what the term hacking means and the motives of hacking.

Early days the word hacker was defined as someone who makes furniture with axe. In the 1960s and 1970 the definition of the word hacker was used to describe a person working with computers who was technically gifted. and the hackers dictionary by (Forestor and Morrison) outline several definition of hacker such as a person who enjoys exploring the detail of programmable systems and how to stretch their capabilities as opposed to most users, who prefer to learn only the minimum necessary, an expert of any kind, a person one who enjoys the intellectual challenge of creativity overcoming or circumventing limitations and so on Now a days this definition is shifted to describe a person who uses a specialised knowledge of computer systems to obtain illegal or unauthorised access to a computer material. The wide popular use of the word hacking more or less eliminated the use of the word hacking for all other purposes and now indicates unauthorised access to a computer material.

Hackers persist of distinguishing them self with crackers, hackers define the term hacker as one who is “ intensely interested in the arcane and recondite working of any computer operation systems” cracker on the other hand is

defined as one who “ breaks into or otherwise violates the system integrity of remote machines, with malicious

What motivates a person to hack can be complex; however the most obvious reasons are recognition, admiration, curiosity, power & Gain and revenge.

Recognition is a desire for fame, most hackers want recognition for their work. The reason behind recognition is human nature most of us would like to have some fame. In some case fame can also bring a financial reward. It is a common practice for hacker to work for security firms and even large accounting firms.

Admiration; is similar to people who become interested in football because they admire a well know or famous footballer. So some individuals who want to learn to hack because they admire hackers.

Curiosity; is for many hackers a driving force behind what they do, most text book put curiosity the number one motivating factor of hackers. That’s way there days many hackers are working in the security industry, making a living doing hacking. If you love teaching wouldn’t you like to be able to make a living as a teacher?

Power & Gain; there has been many instances a hacker appear with a primary goal for power or financial gain. There people don’t necessarily develop there skill for power & gain, when the start it could be just for curiosity or admiration but they can decide later to use there skill toward a particular end to obtain power & financial gain.

Revenge; is when individual feeling wrong done in some way , the hacking can be toward friends, partners, ex partners and some does as far as to state and organisation, so there learn the skill to revenge in many case it is a temporary desire.

Now a day one doesn't have to be computer expert to become a hacker. There are well over 32, 000 hacking oriented websites, they offer easy to use click and hack programs to download. The easy accessibility of hacking materials opened the door for a multitude of new exploits. That's why government in many countries were forced to introduce a new law covering this issue.

The objectives of early hackers are a lot different from some of today's hackers. The most obvious motive of early days hackers were, curiosity, and admiration, some of today's hacker are driven by power and gain, which is in essence greed, revenge and also some after malicious intent, treating hacking as a game or sport employing the tools that are readily available via the internet. Hackers might argue those individual are crackers.

According to the computer misused act (1990), unauthorised access to computer materials, which is seen as a simple hacking that using a computer without permission is criminal offence and also carries an imprisonment penalty of up to six months or a £2000 fine, the individuals are tried in a magistrates court. Unauthorised access to computer material with the intent to commit or facilitate, commission of further offence. This section of the act covers actions such as obtaining bank account or credit card details to commit further crime. Unauthorised modification of computer material, this

part of the act covers altering an account, deletion of files, distributing a computer virus, so on. The 2nd and 3rd section of the act carries up to 5 years imprisonment and also unlimited fine to show the gravity of the crime individuals are tried before jury.

The US's computer fraud and abuse act (1996) is quite the same as UK's act. The major distinction between is two acts are, in the US the penalty can be up to 20 years imprisonment. In particular knowingly accessing computer without or in excess of authority to obtain classified information.

The ACM Code of ethics and professional conduct explicitly state that “ a member must access computer and communication resources only when authorised to do so” and “ avoid harm to others”.

Early days hackers even established their own ethical code, still most hackers claim to stick to a hacker ethic when they hack. These hackers are said to be “ real” hackers of today because they are principled and never damage anything. Their ethic are “ access to computers and anything which might teach you something about the way the world works should be unlimited and total; all information should be free, Mistrust authority promotes decentralisation, hackers should be judged by their hacking not bogus criteria such as academic excellence, age, race or position and you can create art and beautify on a computer”.

So for real hackers defend their action with their ethic and also they argue break-in illustrate security problem to a community that would otherwise not listen

As stated above these days hackers are quite different from early days hackers, it's will stereotyping to say all of hackers these days are driven by greed and revenge. As any profession there are good and bad individuals.

The difference between hacker and cracker is not based on any laws but on the state of mind of the person, there is extremely fine line between hacker and cracker. Today's real hacker can turn in to cracker.