Free essay about cyber crime

Countries, England

Hacking is the unauthorized access of very important information about something or somebody willingly and maliciously for one's personal interests. It is a crime that has been so common from the inception of the internet, this has always been acted in films where people have always brought down big organizations by hacking their very important information and taking control of it (Gibson, 2009). In most countries, this is a criminal offence since it can lead to maliciously getting into the information of a country and causing undue havoc. Hacking does not have any good reason for it, it has always been a malicious way of getting information from sources that are unauthorized. Computer hacking in the United Kingdom is a crime that carries possible sanction of imprisonment especially when you are caught practicing it.

There are several laws that have been set especially in the United Kingdom against hacking. There are several acts that have been formed to deal with computer related actions that are not welcoming. The computer misuse act of 1990 is one of the acts that have been developed to deal with such law breakers (Schwabach, 2013). According to the act, it is illegal to hack into someone's computer or sending people information that through viruses they will enable they have information about someone else without his or her consent. The reason behind the formation of the computer misuse act was the fear that people, especially private investigators would get into peoples accounts to know about something without their consent. Computer hacking in the United Kingdom is a serious act and is always punishable by the law. Its punishment is very serious since it is a crime that leads to another serious offenses such as; fraud, theft among other.

The computer misuse act of the United Kingdom was established in the year 1990 due to a commission from the law that surrounded the misuse of computers and because of the big pressure that the government was receiving from its citizens about the same act. In the act developed in the year 1990, there are three offences that make computer hacking a serious offence. These include; unauthorized access with intent to create some other offenses, unauthorized access to computer material and finally unauthorized modification of the information accessed (Gibson, 2009). Beyond the computer misuse act of 1990, there are other laws that generally deal with hacking in the United Kingdom. The other most common act is the terrorism act 2000. There are several terrorism offenses that were committed which gave rise to this act concluding that hacking is a terrorism offense meaning that anybody found hacking will be judged of terrorism (Gibson, 2009)..

Despite the fact that hacking was regarded a terrorist offense, it could only amount to terrorism under the conditions provided. If the hacking is engineered to influence the government or to get into the public issues or even section of the public, then it could tantamount to a terrorist offense. If it is committed with the main purpose of advancing a political, ideological or even a religious cause, then that could be regarded a terrorism act.

The serious laws that have been set in the united kingdom have to a great extent decreased the acts of hacking into computers, having in mind that there are other offenses that are inscribed in the laws of the United Kingdom that do not contain the same weight that the hacking offense caries, it has made people to fear the act of hacking into information that one does not have due authority over. Before misuse of computer act 1990, and the

terrorism act 2000, there were several criminal offenses that used to happen and someone could go scratch free since it was not put down anywhere in the laws of the United kingdom (Schwabach, 2013). The cases of hacking have reduced by a great percentage in the recent times because of the tight laws that have been enacted in the country about hacking. However, the fight against hacking has not yielded enough fruits because, similar acts still take place in the United Kingdom. The recent case of a journalism hacking into the phone's voicemail in the UK is one of the cases that show how the law has not yet worked satisfactorily in this criminal offense.

The law has got several loopholes in dealing with this crime; the law is becoming lenient to the hackers giving the a reason to continue hacking, several cases have been heard about hacking whose destiny is not known, this shows that the law is becoming so weak in dealing with hacking. Despite the weight given to this criminal offense, its verdict is not equivalent (Gibson, 2009). Terrorism is a serious offense and hacking is equated to it, but the hearing and judgment of the case does not show the seriousness of the offense. In order to effectively deal with hacking, it is very important that the government comes in full swing to tackle this problem. The jury should increase the verdict of those caught in the very act so that the rest can learn from them.

Reference

Gibson, B. (2009). The pocket A-Z of criminal justice. Sherfield Gables, Hampshire, UK: Waterside Press.

Schwabach, A. (2013). Internet and the Law: Technology, Society, and Compromises, Second Edition. Santa Barbara: ABC-CLIO.