Hacking and cracking

The Computer Misuse Act 1990 was introduced in response to a rise in computer hacking. As computers became more commonplace in homes and businesses, the methods by which intrusion and theft took place also changed.

Hacking and cracking have various definitions. Generally, either term can be used to describe an activity that involves trying to gain access to computer systems in order to steal, modify or damage the data that the systems contain. A hacker who illegally attempts to access a computer system can be described as a black-hat hacker.

White-hat hackers, also known as ethical hackers, are computer security experts that attempt to hack computer systems with the permission of the owner. While attempting to hack systems, they look out for security weaknesses and help to put appropriate measures in place to remove these.

Ethics of Hacking and Cracking

An ethic is a standard of right or wrong as per societal norms. Hacking is a technical term that refers to an attempt to successfully gain unauthorized access to a computer website, program, or other resources. On the other hand, cracking involves the action of breaking into a given computer resource such as a system, often for malicious personal objectives (Geisler, 2018). Hacking has rendered cybersecurity one of the most significant issues in the digital industry (Gupta & Anand, 2017). However, hacking can be ethical when a company performs a penetrative action into its systems to test the resources' safety.

Many hackers and crackers are motivated by ill motives to perform malicious actions in systems that are not allowed. First, hackers hack to steal some database of a given company if the files' information is beneficial to them (Geisler, 2018). Hackers manage to steal a company's identity where they open credit accounts, hence ringing up a lot of money. Second, hackers penetrate systems to have control of internet-enabled services.

Hacking and cracking can be ethical if the target company has consent for performing security tasks, and that is referred to as white hat. However, people who engage in unethical hacking violate the cybercrime law and are subject to the prosecutors' legal measures due to the commission of an act classifies as black hat (Gupta & Anand, 2017). Black hat may lead to the loss of resources if the hackers manage to transfer funds into their accounts, leading to a company collapsing due to the loss.

In case computer technicians are authorized to penetrate a company's security testing resources, they should only do that under permission but not every time they wish. It is important to remember that hacking puts data and information to be at risk of malicious usage (Geisler, 2018). Therefore, companies should ensure that adequate security measures are put in place to discourage hackers from gaining access.