

Cybercrime

Student's Name

University Affiliation

Cybercrime

The mounting listing of cybercrimes consists of criminal activities which have actually been facilitated by computers, for instance the dissemination of computer viruses and network intrusions, in addition to computer-based variants of the existing criminal activities, for instance terrorism, bullying, stalking, and identity theft (Wall, 2007). This paper provides a detailed discussion of cybercrime. A definition of the term cybercrime is provided. The paper also describes some of the common sorts of cybercrime.

A cybercrime is understood as any type of crime which involves a network and a computer. In most instances, the computer is utilized by the offender in committing the crime, while in some other instances the computer is utilized by the criminal as the target of criminal activity (Hyman, 2013). Cybercrime is an area of crime that is growing really fast. It is worth mentioning that criminals are increasingly taking advantage of the anonymity, convenience as well as speed of the internet to carry out various crimes which do not know borders whether virtual borders or physical borders, bring about serious damage, and create real threats to victims all over the globe (Interpol, 2016).

There are various sorts of cybercrimes including the following: first is identity theft. In this sort of cybercrime, the offender steals private information of another person and then pretends to be that particular individual so as to get monetary resources in the name of that individual without that person's permission (McMahon, Bressler & Bressler, 2016). The second type is computer viruses. These are essentially malicious computer programs which, after a user opens them, put reproductions of themselves into the hard-drives of the user's computer without the assent of the user. The third type is phishing scams. Herley (2014)

pointed out that these occur when the offender tries to get confidential information like passwords and usernames of other people by acting as if they are a dependable entity in an electronic communication. The fourth type is cyber stalking. In this sort of cybercrime, the offender uses electronics or the internet in harassing or stalking an organization, a person, or a particular group (McMahon, Bressler & Bressler, 2016). In most kinds of cybercrimes, Hyman (2013) reported that the punishment for the criminal is a prison sentence.

New trends in regards to cybercrime are always emerging, with financial costs to the global economy each year estimated to be billions of dollars. Cybercrime was previously carried out largely by small groups of people or by individuals. These days however, there are very extensive networks of cybercriminals bringing together people from various parts of the world in real time to carry out criminal activities on an unparalleled level (Interpol, 2016). Criminal organizations nowadays turn more and more to the internet to aid their crimes and maximize their profits within the shortest time. Even though the criminal activities are not essentially new, for instance of counterfeit medications, illicit gambling, fraud and theft, they are in fact changing consistent with the opportunities presented on the internet. As such, cybercrimes are becoming growingly destructive and extensive (Interpol, 2016).

In conclusion, cybercrime is a sort of crime involving a network and a computer. The computer can be utilized by the offender in committing the crime or the computer could be utilized by the criminal as the target of criminal acts. The main sorts of cybercrime include identity theft, cyber stalking, and phishing scams. The fiscal costs to the global economy associated with cybercrimes each year is billions of dollars.

References

- Herley, C. (2014). Security, Cybercrime, and Scale. *Communications Of The ACM*, 57(9), 64-71. doi:10.1145/2654847
- Hyman, P. (2013). Cybercrime: It's Serious, But Exactly How Serious?. *Communications Of The ACM*, 56(3), 18-20. doi:10.1145/2428556.2428563
- Interpol. (2016, August 29). *Cybercrime*. Retrieved from <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>
- McMahon, R., Bressler, M. S., & Bressler, L. (2016). New global cybercrime calls for hightech cyber-cops. *Journal Of Legal, Ethical & Regulatory Issues*, 19(1), 26-37.
- Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Coventry, England: Prentice Hall.