**NAME: ANELE JEFF**

**MATRIC NO: 19/SCI01/018**

**DEPARTMENT: COMPUTER SCIENCE**

**TOPIC: CYBERCRIME**

**COURSE: COMMUNICATION IN ENGLISH (GST 122)**

**Essay on cybercrime**

Nowadays, computer is used for different purposes depending on the persons skill and wants. When you look at the population of the people who use computers in the world, the number is very surprising. It increases every day and as every second passes, technologies are increasing. Let’s take China for example an article which says “There are nearly 300 million inter users only in China” So with this population of computer and cyber users, there is no wrong in saying cyber and computer crime will keep increasing as it is networked internationally, which makes computer criminals to get access to it easily. As government and Businessmen rely on computers so do criminals.

The first recorded cybercrime was in 1820. This is not surprising because the first form of computer is Abacus which has been around since 3500BC. By looking at this fact there will be no doubt saying that cybercrime will keep increasing day by day.

In technically driven society, people use various devices to make life simple. Globalization results in connecting people all around the world. The increasing access to and continuous use of technology has radically impacted the way in which people communicate and conduct their daily lives. The internet connects people and companies from opposite sides of the world fast, easily, and relatively economically. Nevertheless, the internet and computer can pose some threats which can have disparaging impact on civilizations. Cybercrime is a hazard against different organizations and people whose computers are connected to the internet and particularly mobile technology.

Cybercrime is a dangerous crime involving computers or digital devices, in which a computer can be either a target of the crime, a tool of the crime or contain evidence of the crime. Cybercrime basically defined as any criminal activity that occurs over the Internet. There are many examples such as fraud, malware such as viruses, identity theft and cyber stalking. In present environment, since most information processing depends on the use of information technology, the control, prevention and investigation of cyber activities is vital to the success of the Organizations, Government's agencies and individuals. The procurement and maintenance of highly skill cybercrime expert by Government and Business Enterprises cannot be exaggerated.

Earlier, cybercrime was committed mainly by individuals or small groups. Presently, it is observed that there are highly complex cybercriminal networks bring together individuals at global level in real time to commit crimes.

Today, criminals that indulge in cybercrimes are not motivated by ego or expertise. Instead, they want to use their knowledge to gain profits promptly. They are using their capability to snip, deceive and exploit people as they find it easy to generate money without having to do an honest work. Cybercrimes have become major threat today. Cybercrimes are broadly categorized into three groups such as crime against Individual, Property and Government

Individual cybercrime is the type of cybercrime can be in the form of cyber stalking, distributing, trafficking and "grooming". In present situation, law enforcement agencies are considering such cybercrime very serious and are joining forces worldwide to reach and arrest the committers.

Property cybercrimeis thesame as in the real world where a criminal can steal and pickpocket, even in the cyber world, offenders’ resort to stealing and robbing. In this case, they can steal a person's bank details and drain off money; misuse the credit card to make frequent purchases online; run a scam to get naive people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandal’s damage property in the offline world.

Government cybercrimes against a government are denoted to as cyber terrorism. If criminals are successful, it can cause devastation and panic amongst the citizen. In this class, criminals hack government websites, military websites or circulate propaganda. The committers can be terrorist outfits or unfriendly governments of other nations.

There are a lot of examples involved in cybercrime. A case was filed in which 250,000 was stolen from a Bank in Indonesia through a fake computerized Bank Account. The police in India arrested an unemployed computer operator together with his friend, a host of a five-star hotel allegedly stealing and misusing the total hotel customers credit card numbers. The host copied down the information on the credit card and passes it to his computer operator friend. And what the friend normally does is that he uses the details to purchase a different website online.

Cybercrime can be prevented in so many ways. We can prevent this crime by compromised password, make your password difficult to guess, Profiling, using of random passwords, Malware, by using of Anti-virus, And spyware software. These are the measures to be taken to prevent hackers from intruding into your computer.

Cyber criminals, you will find out that the sentence for a black hat hacker is between 1-5 years in prison. I think if the Government will use these culprits, they can do well to the society by giving them another chance in a community service. And a reasonable punishment should be helping the Government to nab such criminals because they know all the maneuvers involved in hacking or cracking.

In conclusion, what computer and cybercrime will become in the future is not predictable. Things that have been happening before is not what will happen in the future, because every day there is an advancement in the computer world and technology.

There are a lot of cybercrimes victims who refuse to report petty crimes, because they feel what they have lost are too small, they feel it is better to lose than to be embarrassed.

I hope that the people this society will take this case very seriously. Computer crime should be stopped. Reports should be filed immediately no matter how small a crime is because other people may learn from your mistakes.