***ASSIGNEMENT***

***SUBMITTED BY;***

***MUHAMMAD AMJED 32 (2018)***

***SHARJEEL AHMED 33(2018)***

***MUHAMMAD YASIR 29(2018)***

***SHAHAL KHAN 32 (2017)***

***SAAD ULLAH KHAN 37(2018)***

***Saifullah 34(2018)***

***SUBMITTED TO;***

**MAAM UZMA GILANI**

**5TH SEMESTER**

**2018-22**

**MIS**

**TOPIC: CYBERCRIME ACTS**

**Cybercrime Acts:**

Cybercrime is any criminal activity that takes place in the [cyberspace](https://www.voipshield.com/).

One of the earliest and the most common types of cybercrime activity is hacking. It roughly started in the 1960s.

It involves stealing identities and important information, violating privacy, and committing fraud, among others.

According to the Identity Theft Resource Center, over 170 million personal records were exposed through 780 data security breaches in 2015. The global cost of cybercrime is expected to hit $6 trillion by 2021. 30 to 40% of businesses are affected by cybercrime. From 2017 to 2021, businesses are expected to spend more than $1 trillion for cybersecurity.

Every country in the world has their varied laws and rules against cybercrime activities. In the United States, they have substantive cybercrime laws that prohibit identity theft, hacking, intrusion into computers, and child pornography, among others. In the next section, we will determine the most common types of cybercrime activities.

**Most Common Types of Cybercrime Acts**

Cybercrime involves the use of computer and network in attacking computers and networks as well. Cybercrime is obviously a criminal offense and is penalized by the law. Cybercriminals devise various strategies and programs to attack computers and systems. These are the most common types of cybercrime acts:

**Fraud**

Fraud is a general term used to describe a cybercrime that intends to deceive a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing, or suppressing any information to secure unlawful or unfair gain.

**Hacking**

Hacking involves the partial or complete acquisition of certain functions within a system, network, or website. It also aims to access to important data and information, breaching privacy. Most “hackers” attack corporate and government accounts. There are different types of hacking methods and procedures.

**Identity Theft**

Identify theft is a specific form of fraud in which cybercriminals steal personal data, including passwords, data about the bank account, credit cards, debit cards, social security, and other sensitive information. Through identity theft, criminals can steal money. According to the U.S. Bureau of Justice Statistics (BJS), more than 1.1 million Americans are victimized by identity theft.

**Scamming**

Scam happens in a variety of forms. In cyberspace, scamming can be done by offering computer repair, network troubleshooting, and IT support services, forcing users to shell out hundreds of money for cyber problems that do not even exist. Any illegal plans to make money falls to scamming.

**Computer Viruses**

Most criminals take advantage of viruses to gain unauthorized access to systems and steal important data. Mostly, highly-skilled programs send viruses, malware, and Trojan, among others to infect and destroy computers, networks, and systems. Viruses can spread through removable devices and the internet.

**Ransomware**

Ransomware is one of the most destructive malware-based attacks. It enters your computer network and encrypts files and information through public-key encryption. In 2016, over 638 million computer networks are affected by ransomware. In 2017, over $5 billion is lost due to global ransomware.

**DDoS Attack**

DDoS or the Distributed Denial of Service attack is one of the most popular methods of hacking. It temporarily or completely interrupts servers and networks that are successfully running. When the system is offline, they compromise certain functions to make the website unavailable for users. The main goal is for users to pay attention to the DDoS attack, giving hackers the chance to hack the system.

**Botnets**

Botnets are controlled by remote attackers called “bot herders” in order to attack computers by sending spams or malware. They usually attack businesses and governments as botnets specifically attack the information technology infrastructure. There are botnet removal tools available on the web to detect and block botnets from entering your system.

**Spamming**

Spamming uses electronic messaging systems, most commonly emails in sending messages that host malware, fake links of websites, and other malicious programs. Email spamming is very popular. Unsolicited bulk messages from unfamiliar organizations, companies, and groups are sent to large numbers of users. It offers deals, promos, and other attractive components to deceive users.

**Phishing**

Phishers act like a legitimate company or organization. They use “email spoofing” to extract confidential information such as credit card numbers, social security number, passwords, etc. They send out thousands of phishing emails carrying links to fake websites. Users will believe these are legitimate, thus entering their personal information.

**Social Engineering**

Social engineering is a method in which cybercriminals make a direct contact with you through phone calls, emails, or even in person. Basically, they will also act like a legitimate company as well. They will befriend you to earn your trust until you will provide your important information and personal data.

**Malvertising**

Malvertising is the method of filling websites with advertisements carrying malicious codes. Users will click these advertisements, thinking they are legitimate. Once they click these ads, they will be redirected to fake websites or a file carrying viruses and malware will automatically be downloaded.

**Cyberstalking**

Cyberstalking involves following a person online anonymously. The stalker will virtually follow the victim, including his or her activities. Most of the victims of cyberstalking are women and children being followed by men and pedophiles.

**Software Piracy**

The internet is filled with torrents and other programs that illegally duplicate original content, including songs, books, movies, albums, and software. This is a crime as it translates to copyright infringement. Due to software piracy, companies and developers encounter huge cut down in their income because their products are illegally reproduced.

**Child Pornography**

Porn content is very accessible now because of the internet. Most countries have laws that penalize child pornography. Basically, this cybercrime involves the exploitation of children in the porn industry. Child pornography is a $3-billion-a-year industry. Unfortunately, over 10,000 internet locations provide access to child porn.

**Cyberbullying**

Cyberbullying is one of the most rampant crimes committed in the virtual world. It is a form of bullying carried over to the internet. On the other hand, global leaders are aware of this crime and pass laws and acts that prohibit the proliferation of cyberbullying.