Digital Computer Crime

[Name of the Writer]

[Name of the Institution]

Digital Computer Crime

**Introduction**

Times have changed and so have our machines and computers. The growing advancement in technology is benefitting mankind at a large scale. All over the world, computers and computer systems are widely used to carry out millions of operations every second. Computers are being used in every area and every field. From big industries to a small kitchen, every area takes the help of computer and internet to operate.

Along with the numerous blessings that it has brought with itself, technology has also given multiple evils to the world. Criminals have found ways to corrupt the arenas of technology and the internet as well, and various acts of criminal nature are taking place over the internet. Such a kind of crime is known as digital crime. The term digital crime refers to the use of computer and computer networks to carry on illegal activities. The computer involved may be the source or the target of the crime. Digital crime is also known as cybercrime or computer-oriented crime.

Another form or more precisely one of the extensions of digital crime is "Digital Terrorism." Digital Terrorism is defined as the use of computers and information technology in the political motive to cause fear and severe disruption in society (Taylor, Fritsch, & Liederbach, 2014). The acts of digital terrorism or cyber terror include violent acts which may result in the loss of life, creation of terror or fear, significant physical harm or the achievement of political or ideological benefits by the use of threat or intimidation.

This essay will look into the details of the digital crime, digital terrorism and their types prevailing in the society. Moreover, it will also highlight the legal provisions and legal enforcement methods used to encounter the issues of digital crime and digital terrorism.

**Discussion**

We come across many pieces of news regarding digital crimes on a daily basis that have happened in one part of the world or another. One day, the news of a bank robbery through the the internet is making rounds and the other day, some act of terrorism is seen taking place in some other part of the world (Aggarwal, Arora, & Ghai, 2014).

**Types of Digital Crime**

Digital crimes can be classified into the following four major categories:

**Hacking**

Hacking refers to gain illegal and unauthorized access of any device, internet account or computer network. The individuals who involve in the act of hacking are known as hackers.

**Cyber stalking**

The use of internet and multiple other online platforms in order to talk harass or blackmail any person or group is known as cyber stalking. In some cases, cyber stalking can lead to physical violence, rape, and even murder.

**Online identity theft**

The act of stealing personal and confidential information like credit card number, secret pin codes, social security number, bank account number, etc. This can be done by a number of means like phishing, brute force hacking and malware injection.

Online identity theft also refers to using someone else’s identity as your own. For example, using any other person’s information to operate a social media account.

**Internet fraud (Online scams)**

Internet fraud is the act of luring someone into a false situation in which the other person willingly provides their actual and confidential information over the internet, under the belief that they will get a huge benefit in return.

**Most common types of digital crimes**

The most common forms of digital crimes or cybercrime that are taking place all over the world are hacking, internet frauds, online child abuse, online identity theft, ransom ware attack, and cyber stalking.

**Legal provisions**

Cybercrime is a serious criminal offense in the whole world, but the laws and regulations in various countries differ according to the situations. In some countries, the cybercrime laws and legislation are very weak or entirely non-existent, like Philippines. On the other hand, other countries like United States of America and European Union have rigid and well-formulated laws against digital crime where cases of cybercrime are dealt with iron hands, and severe punishments are served for the individuals involved in cybercriminal activities.

In the United States of America, a separate entity deals with the cases of digital crime, known as Federal Bureau of Investigation (FBI), which investigates the cases of digital crime and gets hold of the criminals. One of the examples of the strictness of laws against digital computer crimes is President Obama’s exclusive order to freeze the bank accounts of cyber criminals and block their economic activity within the United States.

**Information systems attacks and countermeasures**

All over the world, there are multiple types of attacks taking place every second. Some of the common cyber-attacks and the countermeasures that are taken to cater these cyber-attacks are listed below.

**Phishing**

One of the most common types of cyber-attacks is Phishing. Phishing refers to sending e-mails that pose to be from some trusted sources, but in actual, they are a part of internet frauds and intended for gaining confidential information from the receiver. There are links provided in such emails which may take the receiver to some other site or may install a malware inside the computer.

The countermeasure to cater the issue of phishing may be to counter check the e-mails before opening, only opening the e-mails that are from trusted sources, carefully analyzing the links in the e-mail and sandboxing the e-mail.

**Malware Attack**

The process of malware attack can be described as when a malicious software gets installed in your system, without the user’s consent. The software gets attached to the applications and programs already existing in the system and may hinder the proper functioning of these applications and programs. It may also replicate and spread in the internal systems of the computer and even harm the hardware of the system.

The most reliable approach to cater the issue of malware attack is the use of a reliable anti-virus. A good antivirus not only detects the malware existing in the computer system, but it also kills and cleanses the system of these malicious software’s. Moreover, it stops further malware from attacking the system by detecting and giving warnings about potentially harmful software before installation.

**Eavesdropping**

The eavesdropping cyber-attack takes place when the network traffic is intercepted and sensitive information, like passwords and credit card number, etc., are extracted out to conduct any burglary or crime further. A person may send confidential information over the internet, and a hacker may get hold of this data actively or passively eavesdropping the network traffic. The best approach to tackle an eavesdropping attack is the encryption of data.

**Information Technology and the Criminal Justice System**

As it has been already established that information technology has taken over every field and every area of work, no matter how big or small, makes use of information technology at almost every level. Just like the other fields, the sector of crime and criminal justice has also advanced and moved to better and much-developed procedures to resolve the criminal offences at a better rate. From the police officers to the judges and parole officers, every individual involved in the criminal justice system is using high-end technology to make the society a crime-free society (Moore, 2014).

**Conclusion**

In a nutshell, although digital crime is a big evil that has engulfed the planet and every second, many people and organizations fall prey to it, but with the help of advanced technology and better techniques to detect and investigate crime, it is becoming easier to catch the lawbreakers. Moreover, the strict laws and regulations also play a significant role in serving justice to the victim at a much better and faster pace.

**References**

Aggarwal, P., Arora, P., & Ghai, R. (2014). Review on cybercrime and security. *International Journal of Research in Engineering and Applied Sciences*, *2*(1), 48-51.

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.