**Internet fundamental and Application**

**11/21/2019**

Ishwor Khatiwada

Cybercrime and its Types

**What is Cybercrime?**

Cybercrime is any criminal activity with the involvement of computer associated with the internet that undergoes as an instrument to further illegal ends, such as committing fraud trafficking in child pornography, phishing, viruses, spyware, ransom ware, intellectual property, stealing identities, or violating privacy.

Hacking was first documented in the 1970s, by then Crime and cybercrime are threats have grown in scope and complexity by each and every day moreover by the advancement in technologies various means of cybercrime have been developed.

Cybercrime is a bigger threat than ever before, now that more and more people are connected to the Internet via laptops, smartphones and smart devices, and is one of the most profitable ways to make money in the criminal world. There are a wide variety of cybercrimes; however they can generally be divided into two categories:

* Crime targeting network or devices.
* Crime using devices to participate in criminal activities.

**Crime targeting network or devices**

Crimes that targets computer networks and smart devices to advance criminal offences can be classified under this category. These types of crimes include viruses and denial-of-service (DoS) attacks, cyber stalking, phishing and fraud or identity theft.

### DDoS Attacks

Distributed Denial of Service (DDoS) attacks are those attacks which focus on the advantage of the specific capacity limits that apply to any network resources such as a company’s website. The DDoS attack will send multiple requests to the attacked web resource with the aim of exceeding the website’s capacity to handle multiple requests and prevent the website from functioning correctly. organization like Internet shopping sites or Any business organization that depends on providing online services are main targeted by these attacks.

**2. Malware**

A malware attack is a common cyber-attack where malware (normally malicious software) executes unauthorized actions on any users system this software are intentionally designed to cause damage to a computer, servers. Different types of malware include viruses, spyware, ransom ware, and viruses Ransom ware, as the name suggests, demands a ransom from you to get things back on track. The main issue with ransom ware, which would spread tremendously fast across organizations and networks.

**3. VIRUSES**

 A virus is a type of computer program that multiplies itself by modifying other computer programs and inserting its own code. It when opened infects gets on the system or comes with attached programs or any data’s that comes from infected webs**.** Some of the most common viruses are:

* Boot Sector Virus
* Direct Action Virus
* Resident Virus
* Multipartite Virus

### Crime using devices to participate in criminal activities

### Identity Theft

### This cybercrime occurs when a criminal gains access to a user’s personal information and access confidential information. They can also open a Sim card/social site account in your name, use your name to plan a criminal activity or sometimes may also claim government benefits in your names. They may do this by finding out user’s passwords through hacking, retrieving personal information from social media that we share, or sending fake emails. For example sending a fake massage of winning a lottery of huge sum of money and by requesting to deposit some money on bank accounts.

### 2. Phishing

### Phishing is a method of tricking user into sharing passwords, credit card numbers, and other sensitive information by posing as a trusted institution via electronic communication.  This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their bank accounts or computer. Users are tricked into emails claiming they need to change their password or update their billing information Etc.

### 3. Cyber stalking

### Communication through social networking sites (Facebook, Whatsapp, Twiter) and other online public platforms can be beneficial, both socially and professionally. However, if users are not careful, it can lead to various consequences, one of which is cyber stalking (harassment). It is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization. However, being monitored by or receiving intrusive messages from an unfamiliar person or a casual acquaintance can be considered cyber stalking. Stalking may be of various motives including blind trust, revenge, anger, or even lust.one of the most common example is fake identity communication in Facebook.