

# Computer law

lec2

# Cyber crimes against property

These crimes include computer vandalism (destruction of others' property ) and transmission of harmful viruses or programs.

# Cyber crimes against property

## 1. Intellectual Property Crimes :

- Intellectual property consists of a bunch of rights.
- Any unlawful act by which the owner is **deprived** completely or partially of his **rights** is a crime.
- The most common type of IPR violation may be said to be **software piracy** , **infringement of copyright**, **trademark** , **patents** , **designs** and **service mark violation**, **theft of computer source code**, etc.

# Cyber crimes against property

## 3- Cyber Vandalism التخريب الإلكتروني:

- Vandalism means deliberately damaging property of another.
- Thus cyber vandalism means **destroying or damaging the data or information stored in computer when a network service is stopped or disrupted.**
- It may include any kind of **physical harm done to the computer** of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral or a device attached to the computer.

# Cyber crimes against property

## 4- Hacking Computer System :

- Hackers attack those included Famous Twitter, blogging platform by **unauthorized access/control** over the computer.
- Due to the hacking activity there will be **loss of data**.
- Also **were not research** especially indicates that those attacks mainly intended for **financial** gain too but they **diminish the reputation** of particular person or company.

# Cyber crimes against property

## 5- Transmitting Virus:

- Viruses are programs written by programmers that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network.
- They mainly affect the **data** on a computer, either by altering or deleting it.

# Cyber crimes against property

## 6- Cyber Trespass:

It means to access someone's computer or network without the right authorization of the owner and **disturb, alter, misuse, or damage data** or system by using wireless internet connection.

# Cyber crimes against property

## 7- Internet Time Thefts:

- It is **the use** by an unauthorized person, of **the Internet hours** paid for by another person.
- The person who gets access to someone else's ISP(internet service provider) user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.
- You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

# **Cyber crimes against government**

# Cyber crimes against government

## Cyber terrorism

The growth of internet has shown that the medium of **Cyberspace** is being used by **individuals and groups** to **threaten the international governments** as also to threaten the citizens of a country.

- This crime manifests itself into terrorism when an individual "cracks" into a **government or military maintained website**.
- When the **European Convention** drafted the Cyber Crime Convention, no exact definition of cyber crime was provided. Every country has its own way of defining cyber crime, which is peculiar to its own socio-cultural situations.

# Cybercrimes Against Society at large

An **unlawful act** done with the intention of causing  
harm to the cyberspace will affect **large number**  
**of persons.**

# Cybercrimes Against Society at large

1. **Child Pornography**: In this act there is use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
2. **Cyber Trafficking**: It involves trafficking in **drugs, human beings, arms weapons** etc. which affects large number of persons.

# Cybercrimes Against Society at large

3. **Online Gambling**: Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. In India a lot of betting and gambling is done on the name of cricket through computer and internet.

4. **Financial Crimes:**

culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.

# Online Fraud

- **Internet Fraud** refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to **conduct fraudulent transactions** or to **transmit the proceeds** of fraud to financial institutions or to others connected with the scheme.

# Online Fraud

## 1- Spam ‘junk mail’ or unwanted messages.

- persuade you to **buy** a product or service,
- **visit a website** where you can make purchases;
- trick you into divulging your **bank account** or credit card details.

## ● 2- Scams :These schemes often arrive uninvited by email.

وتشمل عمليات الاحتيال النigerية تقدم لك حصة (Nigerian Scam) في مبلغ كبير من المال على شرط لك مساعدتها على نقلها خارج بلادهم.

or

إعلانات إبلاغ المستفيدين أنهم قد حصلت مبالغ كبيرة (Lotto Scams) (من المال في اليانصيب الخارجية)

# Online Fraud

3- **Spyware** : software that is **secretly installed on a computer** (without the **permission** or knowledge)

- personal information, business information, bandwidth or processing capacity السعة and secretly gives it to someone else.

4- **Phishing** : is a technique used to gain personal information for the **purpose of identity theft**.

- gain access to people's **online banking details**.
- targeting **online banking customers**,
- **online auction sites**
- **online payment facilities**.

# Online Fraud

## 5- Internet banking fraud

- illegally **remove** money from a bank account
- **transfer** money to an account in a different bank.

## 6- Identity theft

use of personal identifying **information** of an **actual person**, or **fictitious identity** . (either living or dead)

# Suggestions to prevent loss from Online Fraud

- Consideration of using a **low-limit separate credit card for online purchases** to minimize the potential loss if things go wrong.
- **Limiting the amount of personal information** you allow to be ‘the public domain’ i.e.: social networking sites that could be used to assist in identity theft.
- Keeping **anti-virus and firewall** software up to date.

# Crime prevention

- **Crime prevention** Efforts made by governments or people to reduce crime, enforce the law, and maintain criminal justice.
- Several factors must come together for a crime to occur:
  1. individual or group must have the **desire** or motivation to participate in prohibited behavior;
  2. some of the participants must have the **skills** and tools needed to commit the crime;
  3. **opportunity** must be acted upon.

# Crime prevention

1- **Primary prevention** address individual and family level factors correlated with later criminal participation.

- **Individual level** factors such as attachment to **school** and involvement in **pro-social activities** decrease the probability of criminal involvement.
- **Family level** factors such as consistent **parenting skills** similarly reduce individual level risk.

# Crime prevention

- **Secondary prevention** uses techniques focusing on at risk situations such as **youth** who are dropping out of school or getting involved in **gangs**. It targets **social programs** and **law enforcement** at neighborhoods where **crime rates** are high.
- **Tertiary prevention** is used after a crime has occurred in order to **prevent successive incidents**.