# Professional Practices

## “Computer Misuse and The Criminal Law”

# Contents

- Introduction
- Types of Computer misuse
- How to prevent Computer misuse
- Computer misuse and Criminal law
- Real world Cases of Computer Misuse

# Introduction

- Businesses, government and academic institutions are increasingly reliant on the Internet for their day-to-day business, while consumers are using e-commerce more and more for purchasing goods and services.
- All these modern business processes are utilizing computer software and hardware.
- With increased use of computers, there has been a sharp rise in the number of crimes involving computing; and the internet has undoubted create new security risks

# Types of Computer Misuse

- Computer misuse involves the use of computer and network in attacking computers and networks as well.
- 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.

# Types of Computer Misuse

- Some of the most common types of computer misuse are
- **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.

# Types of Computer Misuse

- **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.

# Types of Computer Misuse

- **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.

# Types of Computer Misuse

- **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.

# Types of Computer Misuse

- **Ransomware:** Ransom ware 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 ransom ware. In 2017, over $5 billion is lost due to global ransom ware.

# Types of Computer Misuse

- **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

# Types of Computer Misuse

- **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.

# Types of Computer Misuse

- **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.

# Types of Computer Misuse

- **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.

# Types of Computer Misuse

- **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.

# How to Prevent Computer Misuse???

- The most popular ways to prevent computer misuse are
- **Keep your software updated**
  - This is a critical requirement for any computer system and application. Always keep your OS system, services and applications updated to have the latest bugs and vulnerabilities patched.
  - This advice applies to smart phones, tablets, local desktop computers, notebooks, online servers and all applications they run internally.

# How to Prevent Computer Misuse???

- **Enable your system firewall**
  - Most operating systems include a full pre-configured firewall to protect against malicious packets from both the inside and the outside. A system firewall will act as the first digital barrier whenever someone tries to send a bad packet to any of your open ports.

# How to Prevent Computer Misuse???

- **Use different/strong passwords**
  - Never use the same password on more than one website, and always make sure it combines letters, special characters and numbers.
  - The best way to sort this out is to use a password manager like 1Password, LastPass or Keepass, which will help you generate strong passwords for each website, and at the same time store them in an encrypted database.

# How to Prevent Computer Misuse???

- **Use antivirus and anti-malware software**
  - This is an excellent measure for both desktop and corporate users. Keeping antivirus and anti-malware software up to date and running scans over local storage data is always recommended.
  - While free antivirus/antimalware solutions can be helpful they are often merely trial software, and don't offer full protection against most common virus/malware and other network threats.

# How to Prevent Computer Misuse???

- **Activate your email's anti-spam blocking feature**
  - A lot of computer hacking takes place whenever you open an unsolicited email containing suspicious links or attachments.
  - First enable the anti-spam feature of your email client; and second (and most important) never open links or attachments from unsolicited recipients. This will keep you safe from phishing attacks and unwanted infections.

# How to Prevent Computer Misuse???

- **Shop only from secure and well-known websites**
  - To prevent you from being a victim of man-in-the-middle attacks and crimes against your credit cards or online wallets, first make sure that the site you're shopping on is encrypted with HTTPS.
  - Also make sure you're shopping on a well-known site, such as Amazon, Ebay, Walmart, etc.

# Computer Misuse and Criminal Law

- The Computer Misuse Act 1990 (CMA) is an act of the UK Parliament passed in 1990.
- CMA is designed to frame legislation and controls over computer crime and Internet fraud.
- The legislation was created to
  - Criminalize unauthorized access to computer systems.
  - Deter serious criminals from using a computer in the commission of a criminal offence or seek to hinder or impair access to data stored in a computer

# Computer Misuse and Criminal Law

- CMA introduced three criminal offences
  - Accessing computer material without permission, e.g. looking at someone else's files.
  - Accessing computer material without permission with intent to commit further criminal offences, e.g. hacking into the bank's computer and wanting to increase the amount in your account.
  - Altering computer data without permission, e.g. writing a virus to destroy someone else's data, or actually changing the money in an account.

# Computer Misuse and Criminal Law

- These offences are punishable as follows
  - Offence 1. Up to 6 months' prison and up to £5,000 in fines.
  - Offences 2 and 3. Up to 5 years in prison and any size of fine (there is no limit).

# Real World Cases of Computer Misuse

# WannaCry virus hits the NHS, 2017

- The most widespread cyber attack ever, hackers managed to gain access to the NHS' computer system in mid-2017, causes chaos among the UK's medical system.
- The same hacking tools were used to attack world-wide freight company FedEx and infected computers in 150 countries.
- Ransomware affectionately named "WannaCry" was delivered via email in the form of an attachment.
- Once a user clicked on the attachment, the virus was spread through their computer, locking up all of their files and demanding money before they could be accessed again.
- As many as 300,000 computers were infected with the virus.
- It was only stopped when a 22-year-old security researcher from Devon managed to find the kill switch, after the NHS had been down for a number of days.

# Hackers steal £650 million from global banks, 2015

- For a period of two years, ending in early 2015, a group of Russian-based hackers managed to gain access to secure information from more than 100 institutions around the world.
- The cyber criminals used malware to infiltrate banks' computer systems and gather personal data
- They were then able to impersonate online bank staff to authorise fraudulent transfers, and even order ATM machines to dispense cash without a bank card.
- It was estimated that around £650 million was stolen from the financial institutions in total.

# One billion user accounts stolen from Yahoo, 2013

- In one of the largest cases of data theft in history, Yahoo had information from more than one billion user accounts stolen in 2013.
- Personal information including names, phone numbers, passwords and email addresses were taken from the internet giant.
- Yahoo claimed at the time that no bank details were taken.
- Releasing information of the breach in 2016, it was the second time Yahoo had been targeted by hackers, after the accounts of nearly 500 million users were accessed in 2014.