Computer Misuse

CS449-Professional Issues in Information Technology

Course Instructor: Saeeda Kanwal

Chapter Outcome

After reading this short chapter, you should:

- understand the Computer Misuse Act and how it applies to common offences;
- appreciate the way in which computer fraud is handled at present and the proposals for changes in the law for the future.

INTRODUCTION

In recent years, the public has been much more concerned about the misuse of the internet than about the more general misuse of computers.

Nevertheless, crimes committed using computers form a significant proportion of so-called white collar crime and it has been necessary to introduce legislation specifically aimed at such activities

Cyber Crime

An act against the public good
NOTE: Each statute/Law that defines a crime must specifically explain the conduct that is forbidden by that statute.

No act can be considered a crime

unless it is prohibited by the law

of the place where it is committed and unless the law provides for the punishment of offenders.

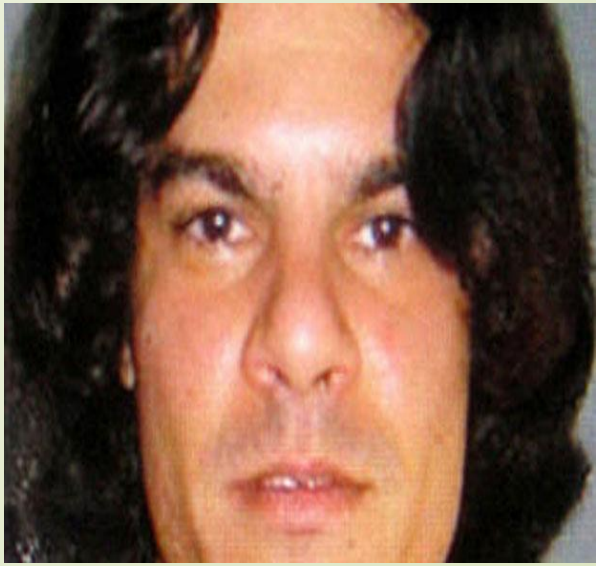
Computer Crime

COMPUTER-RELATED CRIME

Computer crimes refer to the use of information technology for illegal purposes or for unauthorized access of a computer system where the intent is to damage, delete or alter the data present in the computer. Even identity thefts, misusing devices or electronic frauds are considered to be computer crimes.

Top Hackers

- **Kevin Mitnick**
  - (king of all hackers, Los Angeles bus system, Payphones, hacked IBM and Motorola)
- **Albert Gonzalez**
  - (stole 170 million credit card and ATM numbers.)



Top Hackers…..

- **Jonathan James**
  - (stole NASA software estimated at $1.7 million)
- **ASTRA (real name withheld to media)**
  - (Stole weapons technology data and 3D modeling software that he then sold to at least 250 people in Brazil, France, Germany, Italy, South Africa, and the Middle East.)

The Misuse of Computers Act 1990

Categories of Misuse:

- computer fraud;
- unauthorized obtaining of information from a computer;
- unauthorized alteration or destruction of information stored on a computer;
- denying access to an authorized user;
- unauthorized removal of information stored on a computer.

Computer Fraud

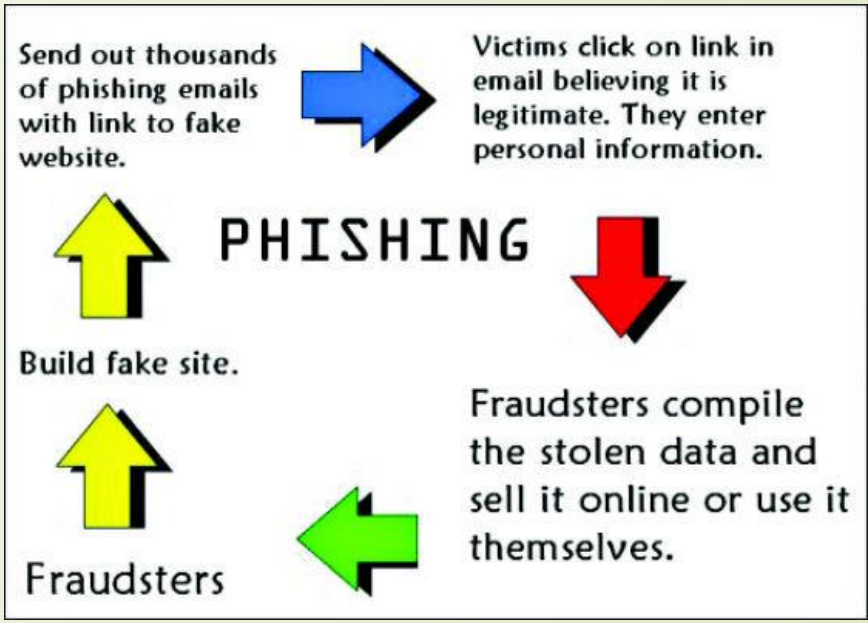
Computer Fraud categories:

- Input fraud
- Output fraud
- Program fraud (salami-slicing)

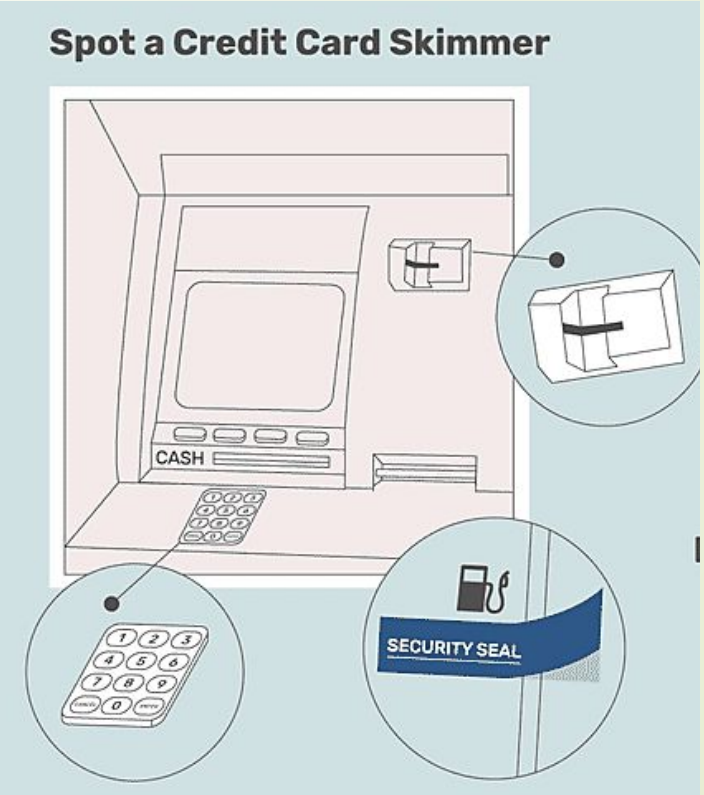
Input Fraud


Income Tax Notice
Fake or Genuine?
NOTICE


TAX
BEWARE! YOUR INCOME TAX NOTICE COULD BE FAKE


Send out thousands of phishing emails with link to fake website.
Victims click on link in email believing it is legitimate. They enter personal information.
PHISHING
Build fake site.
Fraudsters compile the stolen data and sell it online or use it themselves.
Fraudsters

Output fraud



Program fraud (salami-slicing)

Computer Fraud

The Law Commission defined computer fraud as:

. . . conduct that involves the manipulation of a computer, by whatever method, dishonestly obtain money, property, or some other advantage of value, or to cause loss.

The main offences currently covering computer fraud:

- fraud and theft;
- obtaining property by deception;
- false accounting;

Unauthorised Obtaining of Information

The Law Commission identified three particular abuses:

1. computer hacking;
2. eavesdropping on a computer;
3. making unauthorised use of computers for personal benefit.

Historically, it has been difficult to convict anyone of computer hacking.

Unauthorised Obtaining of Information

Under Section 1 of the Computer Misuse Act 1990, a person is guilty of an offence if:

(a) he causes a computer to perform any function with intent to secure access to any program or data held on any computer;

(b) the access he intends to secure is unauthorised;

(c) he knows at the time when he causes the computer to perform the function that this is the case.

SECTION 1: THE MAIN PURPOSE OF THIS SECTION IS TO DETER HACKERS!

SECTION 2: SECTION 1 + FURTHER OFFENCE

Eavesdropping

Eavesdropping involves:

– secret listening;

– secret watching.

The aim is the acquisition of information.

Historically, there has been no right to privacy in the UK.

The recently introduced UK Human Rights Bill incorporates the European Convention on Human Rights into UK law.

Privacy is now recognised as a basic human right. For instance, listening to mobile telephone calls is now illegal.

Eavesdropping….

Most people who misuse computers for personal benefit are in some form of legal relationship with the owner of the computer.

For example, an employee who does private work on their employer's computer.

Here employment law can be applied. The unauthorised use of the computer is not a special issue.

Unauthorised Altering or destruction of Information

Computers store vast amounts of information about us:

- what we have in the bank;
- who we call on the telephone;
- what we buy in the shops;
- where we travel;

Criminals who alter or destroy such information can be dealt with by

- the law on Criminal Damage;
- the Computer Misuse Act 1990 section 3

Unauthorised destruction of Information

The law on Criminal Damage seems to apply to physically stored data for example:

- Damage or Delete data belonging to someone
- writing a program that damages the data on a hard disk.

But not:

- switching off a monitor so that the display can't be seen.

Unauthorised Modification

Section 3 of the Computer Misuse Act 1990 provides that a person is guilty of a criminal offence if:

(a) he does any act which causes unauthorised modification of the contents of a computer, and

(b) at the time when he does the act, he has the requisite intent and the requisite knowledge.

The requisite intent is an intent to cause a modification to the contents of any computer and by doing so:

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program

(c) to impair the operation of any such program or the reliability of any such data.

Forgery

The unauthorised alteration or destruction of data may amount to forgery.

The Forgery and Counterfeiting Act 1981 says:

A person is guilty of forgery if he makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it, to do or not to do some act to his own or any other person's detriment.

Forgery

An “instrument” is usually a written document.

However, it can also be “any disk, tape, sound-track or other device on which information is stored by mechanical, electronic or other means.”

E.g. A forged electronic mail message.

Denying Access to an Authorised User

There are many ways to deny access to an authorised user of a computer:

- shut the machine down;
- overload the machine with work;
- tie up all the machine's terminal/network connections;
- encrypt some system files….etc;

Various offences deal with:

- hacking;
- unauthorised obstruction of electricity;
- improper use of telecommunications services;
- unauthorised modification of computer material;

Unauthorised removal of Info. stored on a computer.

Under the Theft Act 1968, only property can be stolen, and information is not property.

A floppy disk is protected by law, but the information stored on it is not.

Examples 1

Scenario 1

- A student hacks into a college database to impress his friends - unauthorised access
- Later he decides to go in again, to alter his grades, but cannot find the correct file - unauthorised access with intent...
- A week later he succeeds and alters his grades - unauthorised modification of data

Examples 2

Scenario 2

- An employee who is about to be made redundant, finds the Managing Director's password; logs into the computer system using this and looks at some confidential files- unauthorised access
- Having received his redundancy notice he goes back in to try and cause some damage but fails to do so - unauthorised access with intent...
- After asking a friend, he finds out how to delete files and wipes the main customer database - unauthorised modification

Reasons for Cyber Crime not being reported

It is tough to punish a Cyber-crime criminal because:

- Offences are difficult to prove
- Evidences are difficult to collect - firms usually do not cooperate with the police
- Firms are embarrassed or scared about their reputation due to hacking - particularly banks
- Employees are normally sacked or demoted
- Police lack expertise; time; money
- The Cyber-Crime is perceived as ‘soft crime’, as no one gets physically injured or hurt

Current situation

- Hacking has increased with time, both as a prank and as a professional crime
- A few high profile cases are reported in the past
- Offenders are often in other countries with no equivalent legislation
- Some ‘international task forces’ set up but no real progress

Pakistan Cyber Crime Bill-2016

Cyber Laws in Pakistan

- There are different law are promulgated in Pakistan.
- These laws not only deal with crime of Internet
- These deal with all dimensions related to computer & networks.
- Two of them are most known.
- They are:
  - Electronic Transaction Ordinance 2002
  - Electronic / Cyber Crime Bill 2007

Electronic Transaction Ordinance 2002

- Overview
  - The Electronic Transactions Ordinance (ETO), 2002, was the first IT-relevant legislation created by national lawmakers.
  - A first step and a solid foundation for legal sanctity and protection for Pakistani e-Commerce locally and globally.
  - Laid the foundation for comprehensive Legal Infrastructure.
  - It is heavily taken from foreign law related to cyber crime.

Electronic/ Cyber Crime Bill 2007

Overview

- "Prevention of Electronic Crimes Ordinance, 2007" is in force now
- It was promulgated by the President of Pakistan on the 31st December 2007
- The bill deals with the electronic crimes included:
  - Cyber terrorism
  - Data damage
  - Electronic fraud
  - Electronic forgery
  - Unauthorized access to code
  - Cyber stalking
  - Cyber Spaming

Statistics-2015

Offence	Imprisonment (years)	Fine
Criminal Access	3	3 Lac
Criminal Data Access	3	3 Lac
Data Damage	3	3 Lac
System Damage	3	3 Lac
Electronic Fraud	7	7 Lac
Electronic Forgery	7	7 Lac
Misuse of Device	3	3 Lac
Unauthorized access to code	3	3 Lac
Malicious code	5	5 Lac
Defamation	5	5 Lac
Cyber stalking	3	3 Lac
Cyber Spamming	6 months	50,000
Spoofing	3	3 Lac
Pornography	10	-----
Cyber terrorism	Life	10 Million

Sections

- Data Damage:
  - Whoever with intent to illegal gain or cause harm to the public or any person, damages any data, shall come under this section.
- Punishment:
  - 3 years
  - 3 Lac

- Electronic fraud:
  - People for illegal gain get in the way or use any data, electronic system or device or with intent to deceive any person, which act or omissions is likely to cause damage or harm.
- Punishment:
  - 7 years
  - 7 Lac

- Electronic Forgery:
  - Whoever for unlawful gain interferes with data, electronic system or device, with intent to cause harm or to commit fraud by any input, alteration, or suppression of data, resulting in unauthentic data that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not.
- Punishment:
  - 7years
  - 7 Lac

- Spamming:
  - Whoever transmits harmful, fraudulent, misleading,
  - illegal or unsolicited electronic messages in bulk to any person
  - without the express permission of the recipient,
  - involves in falsified online user account registration or falsified domain name registration for commercial purpose commits the offence of spamming.
- Punishment:
  - 6 month
  - 50,000

Special Agency

- Federal Intelligence Agency
  - NR3C

  (National Response Center for Cyber Crimes)
- Sindh Police –Cyber Cop

www.nr3c.gov.pk/index.html

Apps NeON OC-NEON Google Gmail NU Mail HotMail SLATE NU-Khi NU Library Time Diction Save from OneDrive Dropbox NU G-Dr G-Dr

FEDERAL INVESTIGATION AGENCY

NATIONAL RESPONSE CENTRE FOR CYBER CRIME

HOME | ABOUT US | SERVICES | CYBER CRIME | REPORT CYBER CRIME | FAQ | CONTACT US

www.nr3c.gov.pk/index.html

Apps NeON OC-NEON Google Gmail NU Mail HotMail SLATE NU-Khi NU Library Time Diction Save from OneDrive Dropbox NU G-Dr G-Dr

FEDERAL INVESTIGATION AGENCY

NATIONAL RESPONSE CENTRE FOR CYBER CRIME

HOME | ABOUT US | SERVICES | CYBER CRIME | REPORT CYBER CRIME | FAQ | CONTACT US

STEALING DATA IS AN OFFENSE,

UPDATE ANTIVIRUS FOR DEFENSE

www.nr3c.gov.pk/index.html

Apps NeON OC-NEON Google Gmail NU Mail HotMail SLATE NU-Khi NU Library Time Diction Save from OneDrive Dropbox NU G-Dr G-Dr

FEDERAL INVESTIGATION AGENCY

NATIONAL RESPONSE CENTRE FOR CYBER CRIME

HOME | ABOUT US | SERVICES | CYBER CRIME | REPORT CYBER CRIME | FAQ | CONTACT US

Reference

The Computer Misuse Act is available from the website:

www.hmso.gov.uk/acts.htm#acts

National Response Centre for Cyber Crime(Pak):

http://www.nr3c.gov.pk/

Cyber Scout(Pak):

http://www.nr3c.gov.pk/cscouts.html

Prevention of Electronic Crimes Act 2016 (PECA-2016)

Pakistan Cyber Crime Bill-2016

Adobe Acrobat Document

Adobe Acrobat Document