Unit II - Cybercrime and Cyber Offences

Content

- Introduction to Cybercrime:
- Definition and Origins of the Word
- Cybercrime and Information Security
- Cybercriminals
- Classifications of Cybercrimes

- Introduction to Cyber Offences
- Phases of cybercrime used by Criminals
- Social Engineering
- Cyberstalking
- Cybercafe and Cybercrimes
- Botnets
- Attack Vector
- Cybercrime and Cloud Computing

1.1 INTRODUCTION

- The internet in India is growing rapidly.
- It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education.

- There’re two sides to a coin. Internet also has it’s own disadvantages as Cyber crime- illegal activity committed on the internet.

1.1 INTRODUCTION

- “Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber attacks”.
- “Cybersecurity” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
- Almost everyone is aware of the rapid growth of the Internet. Given the unrestricted number of free websites, the Internet has opened a new way of exploitation known as cybercrime.
- These activities involve the use of computers, the Internet, cyberspace and the worldwide web (WWW).

1.2 DEFINING CYBER CRIME

- Crime committed using a computer and the internet to steal data or information.
- Illegal imports or Malicious programs.
- Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.
- There are also stories/news of other attacks; for example, according to a story posted on 3 December 2009, a total of 3,286 Indian websites were hacked in 5 months – between January and June 2009.

- Various cybercrimes and cases registered under cybercrimes by motives and suspects in States and Union Territories (UTs).

Cybercrime

- Cybercrime is not a new phenomena
- The first recorded cybercrime took place in the year 1820.
- *In 1820, JosephMarie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics.*
- *This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened.*
- *They committed acts of sabotage to discourage Jacquard from further use of the new technology.* ***This is the first recorded cyber crime!***

Alternative definitions for cybercrime

- Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution.
- Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
- Any financial dishonesty that takes place in a computer environment.
- Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom.

Another definition

- "*Cybercrime (computer crime) is any illegal behaviour, directed by means of electronic operations, that target the security of computer systems and the data processed by them*".
- Hence cybercrime can sometimes be called as *computer-related crime, computer crime, E-crime, Internet crime, High-tech crime….*

Cybercrime specifically can be defined in number of ways…

- A crime committed using a computer and the internet to steal a person's identity(identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.
- Crimes completed either on or with a computer.
- Any illegal activity through the Internet or on the computer.
- All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.

Cybercrimes

- According to one information security , cybercrime is any criminal activity which uses network access to commit a criminal act .
- Cybercrime may be internal or external, with the former easier to perpetrate.
- The term “cybercrime” has evolved over the past few years since the adoption of Internet connection on a global scale with hundreds of millions of users .
- Cybercrime refers to the act of performing a criminal act using cyberspace as the communications vehicle.

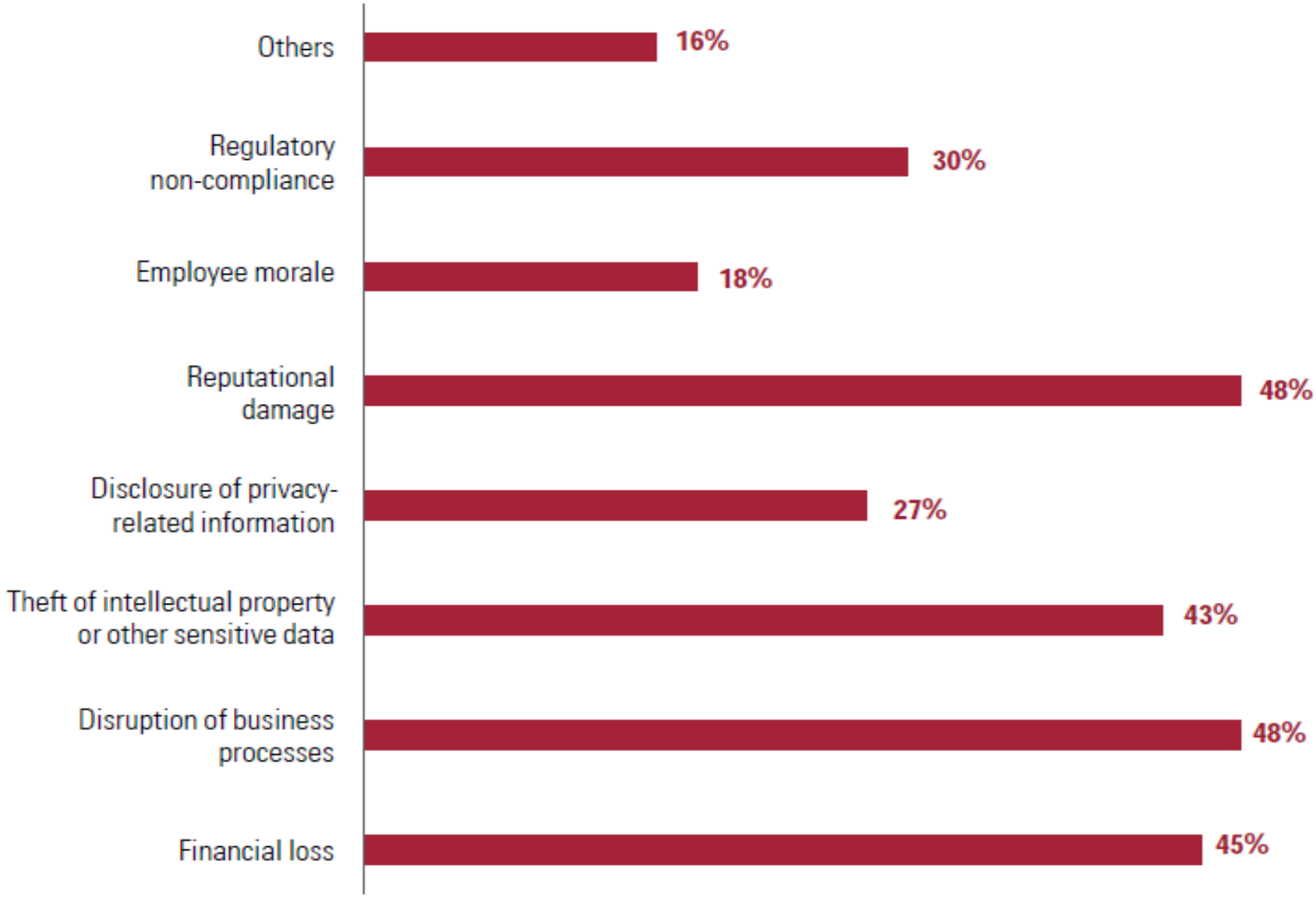
Types of Attacks

- Some people may argue that cybercrime is a crime against computer and not humans, however the legal systems around the world scramble to introduce laws to combat cyber criminals.
- Two types of attacks are prevalent:
  - Techno- crime : *Active attack*
    - Techno Crime is the term used by law enforcement agencies to denote criminal activity which uses (computer) technology, not as a tool to commit the crime, but as the subject of the crime itself.
    - Techno Crime is usually pre-meditated and results in the *deletion, corruption, alteration, theft or copying of data on an organization's systems*.
    - Techno Criminals will usually probe their prey system for weaknesses and will almost always leave an electronic 'calling card' to ensure that their pseudonym identity is known.

Types of Attacks

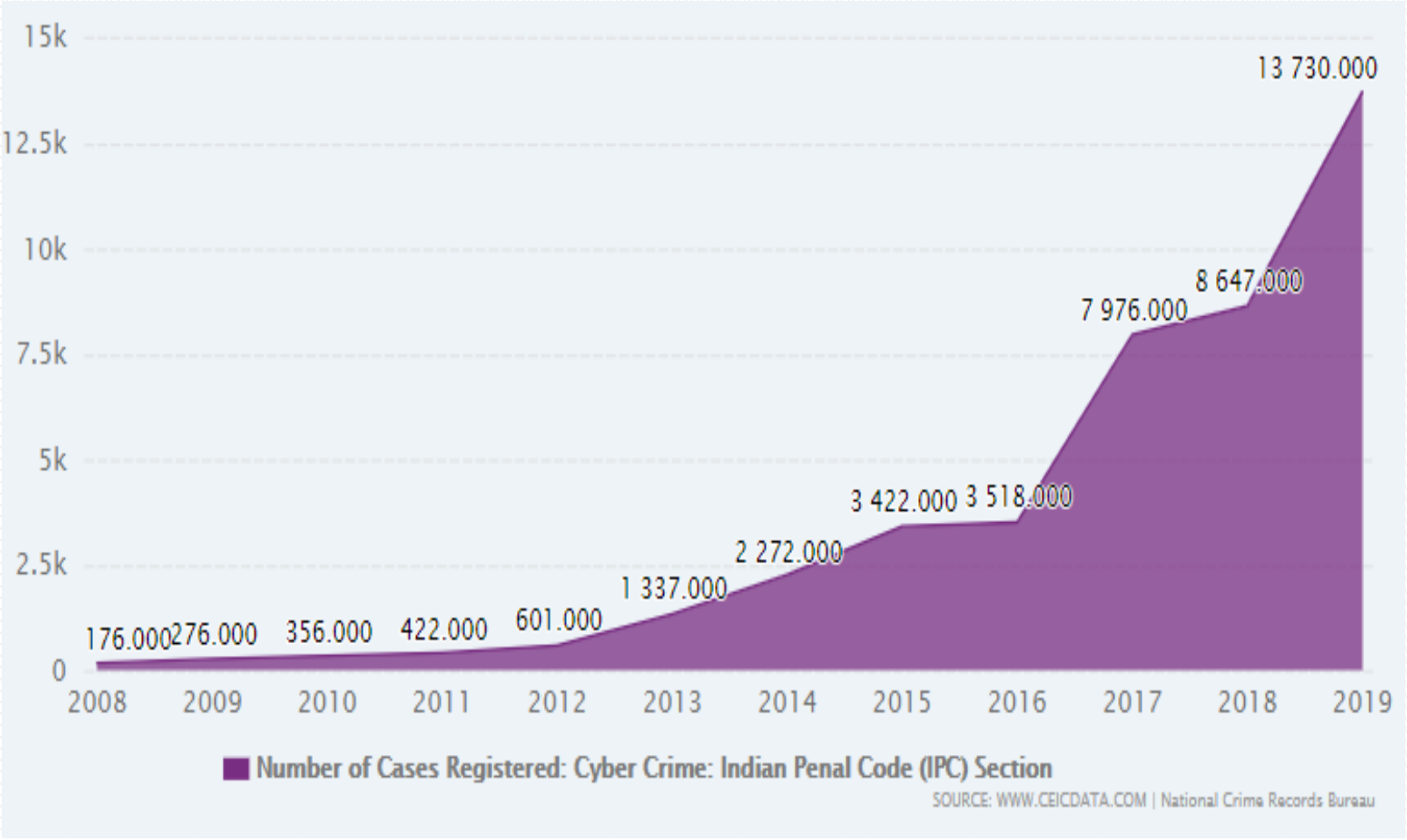
- Techno – vandalism: Passive attack
  - Techno Vandalism is a term used to describe *a hacker or cracker* who breaks into a computer system with the *sole intent of defacing and or destroying its contents*.
  - Techno Vandals can deploy *'sniffers'* on the Internet to locate soft (insecure) targets and then execute a range of commands using a variety of protocols towards a range of ports. If this sounds complex - it is!
  - The best weapon against such attacks is a firewall which will hide and disguise your organization's presence on the Internet.

Survey result - Impact of cybercrime in India



Source: Cybercrime survey report 2014, KPMG in India

Number of cyber crimes reported under IPC section in India from 2008 to 2019



Cybercrime

- Cybercrime: (harmful acts committed from or against a computer or network) differ from most crimes in four ways:
- (a) how to commit them is easier to learn,
- (b) they require few resources relative to the potential damage caused,
- (c) they can be committed in a jurisdiction without being physically present in it
- (d) they are often not clearly illegal.
- The term cybercrime has some stigma attached and is notorious due to the word “terrorism” or
- “terrorist” attached with it, that is, cyberterrorism (see explanation of the term in Box 1.1).

Important Definitions related to Cyber Security

- Cyberterrorism
- Cyberterrorism is defined as “any person, group or organization who, with terrorist intent, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism.”
- Cybercrime, especially through the Internet, has grown in number as the use of computer has become central to commerce, entertainment and government.
- The term cyber has some interesting synonyms: fake, replicated, pretend, imitation, virtual, computer generated.
- Cyber means combining forms relating to Information Technology, the Internet and Virtual Reality.

Important Definitions related to Cyber Security

- Cybernetics
- This term owes its origin to the word “cybernetics” which deals with information and its use; cybernetics is the science that overlaps the fields of neurophysiology, information theory, computing machinery and automation.
- Worldwide, including India, cyberterrorists usually use computer as a tool, target for their unlawful act to gain information.
- Internet is one of the means by which the offenders can gain priced sensitive information of companies, firms, individuals, banks and can lead to intellectual property (IP) crimes, selling illegal articles, pornography/child pornography, etc.
- This is done using methods such as Phishing, Spoofing, Pharming, Internet Phishing, wire transfer, etc. and use it to their own advantage without the consent of the individual.

Important Definitions related to Cyber Security

- Phishing
- Refers to an attack using mail programs to deceive or coax (lure) Internet users into disclosing confidential information that can be then exploited for illegal purposes.
- Figure 1.2 shows the increase in Phishing hosts.
- -

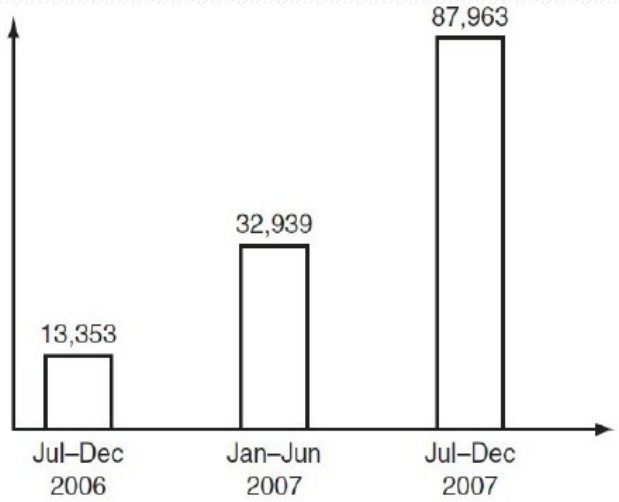
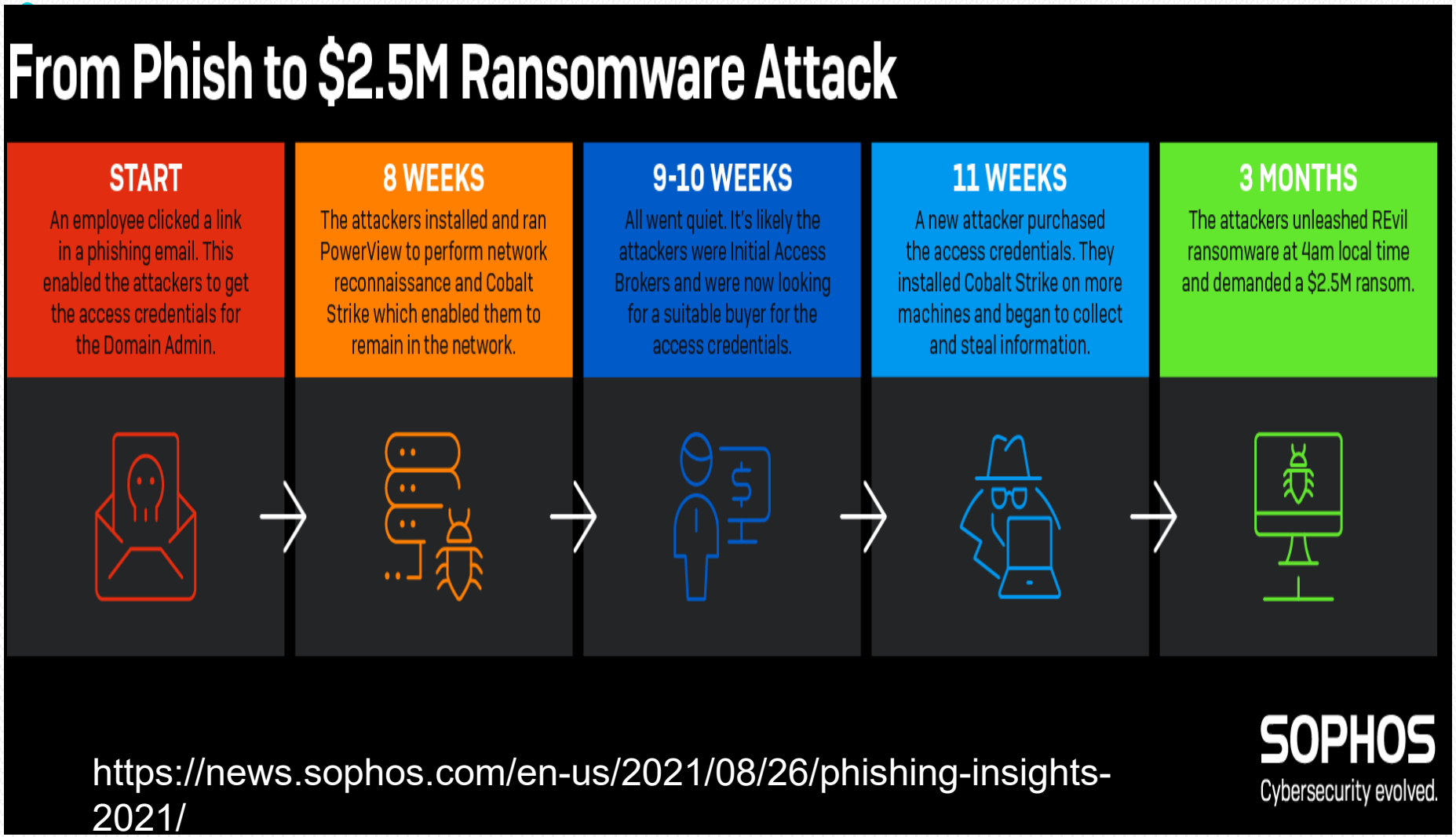


Figure 1.2 Rise in the number of Phishing hosts.
Source: Symantec (International Telecommunications Society, 17th Biennial Conference, Montreal, Canada, June 24–27, 2008).

Important Definitions related to Cyber Security

- Phishing



https://news.sophos.com/en-us/2021/08/26/phishing-insights-2021/

Important Definitions related to Cyber Security

- Phishing

Important Definitions related to Cyber Security

- Cyberspace
- “Cyberspace” is where users mentally travel through matrices of data. Conceptually, “cyberspace” is the “nebulous place” where humans interact over computer networks.
- The term “cyberspace” is now used to describe the Internet and other computer networks .
- In terms of computer science, “cyberspace” is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data.
- Cyberspace is most definitely a place where you chat, explore, research and play.

Important Definitions related to Cyber Security

- Cybersquatting
- The term is derived from “squatting” which is the act of occupying an abandoned space/building that the user does not own, rent or otherwise have permission to use.
- Cybersquatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cybersquatters through the registration process.
- Cybersquatters usually ask for prices far greater than those at which they purchased it.
- Some cybersquatters put up derogatory or defamatory remarks about the person or company the domain is meant to represent in an effort to encourage the subject to buy the domain from them.

Important Definitions related to Cyber Security

- Cybersquatting
- This term relates to cybercrime given the intent of cybersquatting.
- Cybersquatting means registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark.
- In this nature, it can be considered to be a type of cybercrime.
- Cybersquatting is the practice of buying "domain names" that have existing businesses names.
- Cyberpunk
- According to science fiction literature, the words "cyber" and "punk" emphasize the two basic aspects of cyberpunk: "technology" and "individualism."
- The term "cyberpunk" could mean something like "anarchy via machines" or "machine/computer rebel movement."
- (A writer of science fiction set in a lawless subculture of an oppressive society dominated by computer technology)

Important Definitions related to Cyber Security

- Cyberwarfare
- Cyberwarfare means information attacks against an unsuspecting opponent's computer networks, destroying and paralysing nations.
- This perception seems to be correct as the terms cyberwarfare and cyberterrorism have got historical connection in the context of attacks against infrastructure.
- The term "information infrastructure" refers to information resources, including communication systems that support an industry, institution or population.
- These type of Cyberattacks are often presented as threat to military forces and the Internet has major implications for espionage and warfare.

National Crime Records Bureau

- The National Crime Records Bureau was established in 1986 as a repository of information on crime and criminals based on the recommendations of the Tandon Committee, the National Police Commission (1977–1981) and the Task Force of the Ministry of Home Affairs (1985).
- In 2009, the National Crime Records Bureau was entrusted with the responsibility of monitoring, coordinating and implementing the Crime and Criminal Tracking Network and Systems (CCTNS) project. This project in the country connects about 15000 police stations and 6000 higher offices of the country.
- The bureau also launched National Digital Police Portal on 21.08.2017 under CCTNS project.
- https://ncrb.gov.in/

Patterns of Cases Reported and Persons Arrested under IT Act during 2013 – 2015 and Percentage Variation during 2015 over 2014

SL	Crime heads under IT Act	Cases Registered			% Var.	Persons Arrested			% Var.
		2013	2014	2015		2013	2014	2015	
1	Tampering Computer Source Documents (Sec. 65 of IT Act)	137	89	88	-1.1	59	64	62	-3.1
2	Computer Related Offences(Sec. 66 to 66E of IT Act)	2,516	5,548	6,567	18.4	1,011	3,131	4,217	34.7
3	Cyber Terrorism@(Sec. 66F of IT Act)	-	5	13	160.0	-	0	3	-
4	Publication/Transmission of Obscene/Sexually Explicit Content(Sec. 67 to 67C of IT Act)	1203	758	816	7.7	737	491	555	13
5	Intentionally not Complying with the Order of Controller(Sec. 68 of IT Act)	13	3	2	-33.3	3	4	3	-25
6	Failure to Provide or Monitor or Intercept or Decrypt Information(Sec. 69 of IT Act)	6	2	0	-100	7	0	0	-
7	Failure to Block Access any Information Hosted etc.@ (Sec. 69A of IT Act)	-	1	0	-100	-	0	0	-
8	Not Providing Technical Assistance to Govt. to Enable Online Access@(Sec. 69B of IT Act)	-	0	3	-	-	0	0	-
9	Un-authorized Access/Attempt to Access to Protected Computer System(Sec. 70 of IT Act)	27	0	8	-	17	0	4	-
10	Misrepresentation/Suppression of Fact for Obtaining License etc. (Sec. 71 of IT Act)	12	5	4	-20	14	13	2	-84.6
11	Breach of Confidentiality/Privacy(Sec. 72 of IT Act)	93	16	20	25	30	13	6	-53.8
12	Disclosure of Information in Breach of Lawful Contract@(Sec. 72A of IT Act)	-	2	4	100	-	5	2	-60
13	Publishing/Making Available False Elect. Signature Certificate (Sec. 73 of IT Act)	4	0	3	-	8	0	0	-
14	Create/Publish/Make Available Electronic Signature Certificate for Unlawful Purpose(Sec. 74 of IT Act)	71	3	3	0	51	5	3	-40
15	Others	274	769	514	-33.2	161	520	245	-52.9
Total Offences under IT Act		**4,356**	**7,201**	**8,045**	**11.7**	**2,098**	**4,246**	**5,102**	**20.2**

Note: '-' implies sezo value in previous year. % Var. – refers the Percentage Variation during 2015 over 2014
"@ implies data collected in 2014 for the first time

Table 1.1

Table-18 (B)

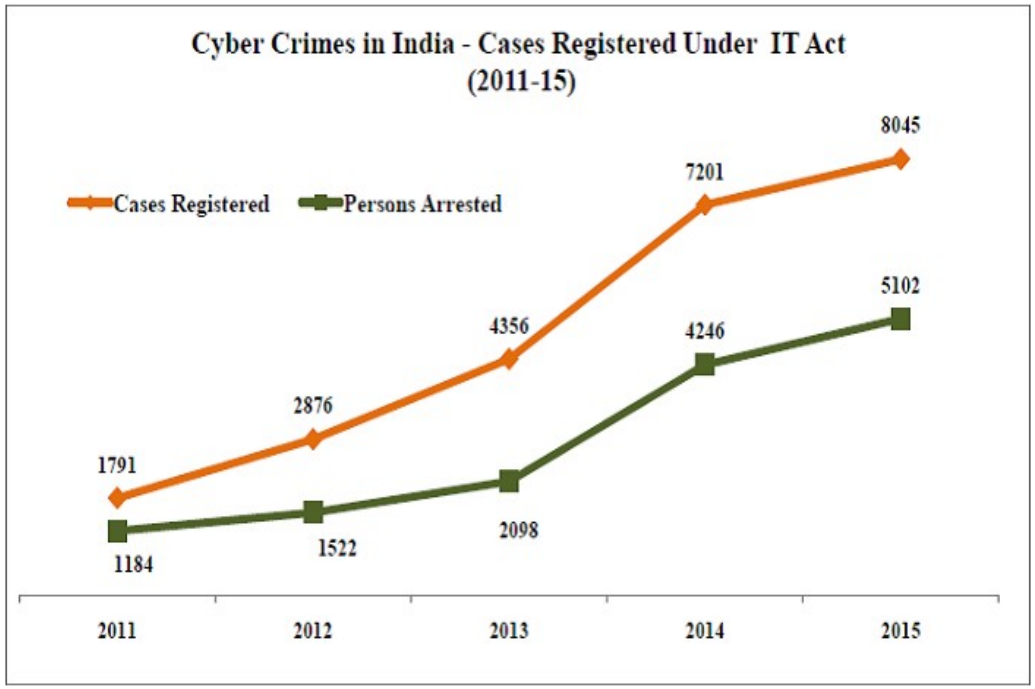
Cyber Crimes/Cases Registered and Persons Arrested under IPC during 2013-2015

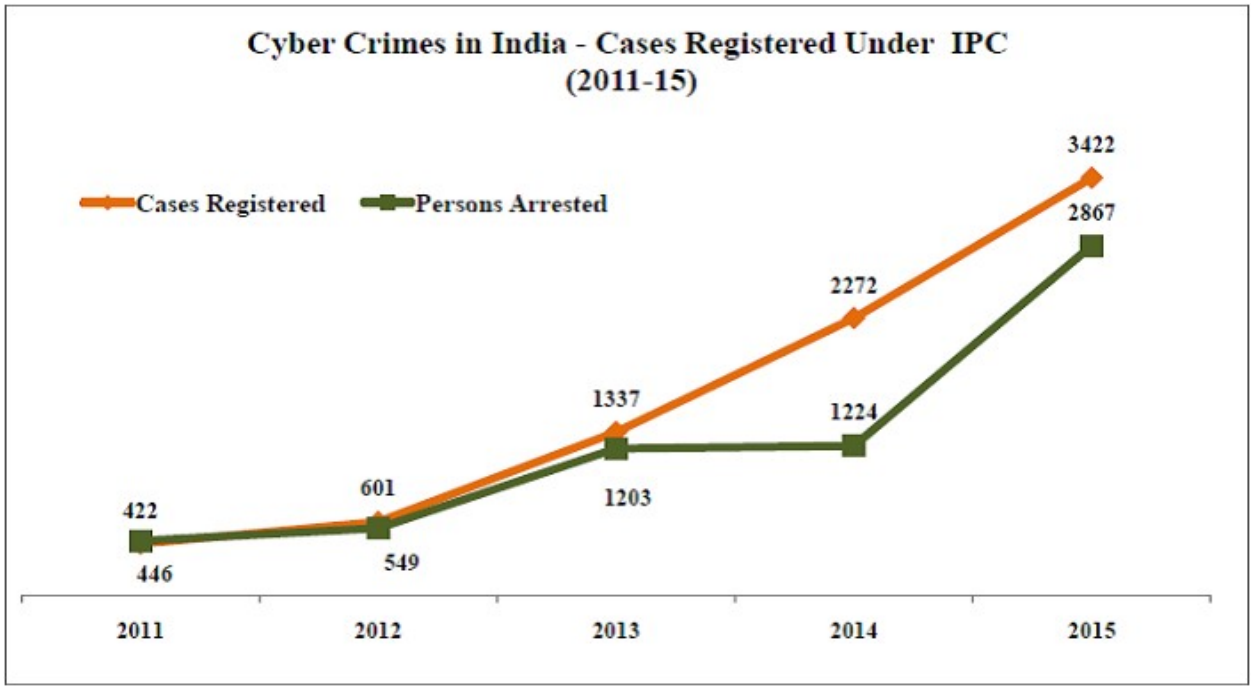
Sl. No	Crime Heads under IPC Crimes	Cases Registered			% Var.	Persons Arrested			% Var.
		2013	2014	2015		2013	2014	2015	
1	Offences by Public Servant	1	0	0	-	2	0	0	-
2	Fabrication/Destruction of Electronic Records for Evidence	12	1	4	300.0	11	1	2	50.0
3	Cheating@	-	1,115	2,255	102.2	-	335	754	55.6
4	Forgery	747	63	45	-28.6	626	58	72	19.4
5	Data Theft@	-	55	84	52.7	-	11	135	91.9
6	Criminal Breach of Trust	518	54	42	-22.2	471	39	1,292	97
7	Counterfeiting *	59	10	12	20.0	93	8	14	42.9
8	Others	-	974	980	0.6	-	772	598	-29.1
Total Offences under IPC		**1,337**	**2,272**	**3,422**	**50.6**	**1,203**	**1,224**	**2,867**	**57.3**

Note * includes property marks, tampering and currency/stamps till 2014 and currency & stamps during 2015
Note: " -" in the column of percentage variation implies zero value in previous year
"@" implies newly entered crime heads. '% Var.' – refers to Percentage Variation in 2015 over 2014

Table 1.2

https://ncrb.gov.in/en/crime-in-india-table-addtional-table-and-chapter-contents?field_date_value%5Bvalue%5D%5Byear%5D=2020&field_select_table_title_of_crim_value=20&items_per_page=All


Cyber Crimes in India - Cases Registered Under IT Act
(2011-15)
Cases Registered
Persons Arrested
1791
2876
4356
7201
8045
1184
1522
2098
4246
5102
2011
2012
2013
2014
2015


Cyber Crimes in India - Cases Registered Under IPC
(2011-15)
Cases Registered
Persons Arrested
422
601
1337
2272
3422
446
549
1203
1224
2867
2011
2012
2013
2014
2015

1.3 Cybercrime and information security

- Lack of information security give rise to cybercrime.
- Let us refer to the amended Indian Information Technology Act (ITA) 2000 in the context of cybercrime.
- From an Indian perspective, the new version of the Act (referred to as ITA 2008) provides a new focus on "Information Security in India."
- Cybersecurity: means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
- The term incorporates both the physical security of devices as well as the information stored therein.

1.3 Cybercrime and information security

- It covers protection from unauthorized access, use, disclosure, disruption, modification and destruction.
- Where financial losses to the organization due to insider crimes are concerned (e.g., leaking customer data), often some difficulty is faced in estimating the losses because the financial impacts may not be detected by the victimized organization and no direct costs may be associated with the data theft.
- The 2008 CSI Survey on computer crime and security supports this.

1.3 Cybercrime and information security

- In an attempt to avoid negative publicity, most organizations abstain from revealing facts and figures about “security incidents” including cybercrime.
- In general, organizations perception about “insider attacks” seems to be different than that made out by security solution vendor.
- However, this perception of an organization does not seem to be true as revealed by the 2008 CSI Survey.
- Awareness about “data privacy” too tends to be low in most organizations.
- When we speak of financial losses to the organization and significant insider crimes, such as leaking customer data, such “crimes” may not be detected by the victimized organization and no direct costs may be associated with the theft (Table 1.5).

Cybercrime trends over years

Table 1.5 | Cybercrime trend over the years (1999–2008)

Types of Cybercrime	*2004 (%)*	*2005 (%)*	*2006 (%)*	*2007 (%)*	*2008 (%)*
Denial of service (DoS)	39	32	25	25	21
Laptop theft	49	48	47	50	42
Telecom fraud	10	10	8	5	5
Unauthorized access	37	32	32	25	29
Viruses (addressed in Chapter 4)	78	74	65	52	50
Financial fraud	8	7	9	12	12
Insider abuse	59	48	42	59	44
System penetration	17	14	15	13	13
Sabotage	5	2	3	4	2
Theft/loss of proprietary information	10	9	9	8	9
• from mobile devices					4
• from all other sources					5
Website defacement (see Figs. 1.6–1.10)	7	5	6	10	6
Abuse of wireless network	15	16	14	17	14
Misuse of web application	10	5	6	9	11

Challenges for securing data in business perspective

- Financial losses to the organization are difficult to estimate because they may not be detected by the victimized organization in case of Insider attacks : such as leaking customer data.
- Cybercrime occupy an important space in information security due to their impact.
- Most organizations do not incorporate the cost of the vast majority of computer security incidents into their accounting.
- The difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost.
- So reporting of financial losses remains approximate.
- Following figure shows several categories of incidences – viruses, insider abuse, laptop theft, unauthorised access to systems, etc.

Cybercrime trends over years

Figure 1.4 shows several categories of incidences – *viruses*, *insider abuse*, *laptop theft* and *unauthorized access* to systems.

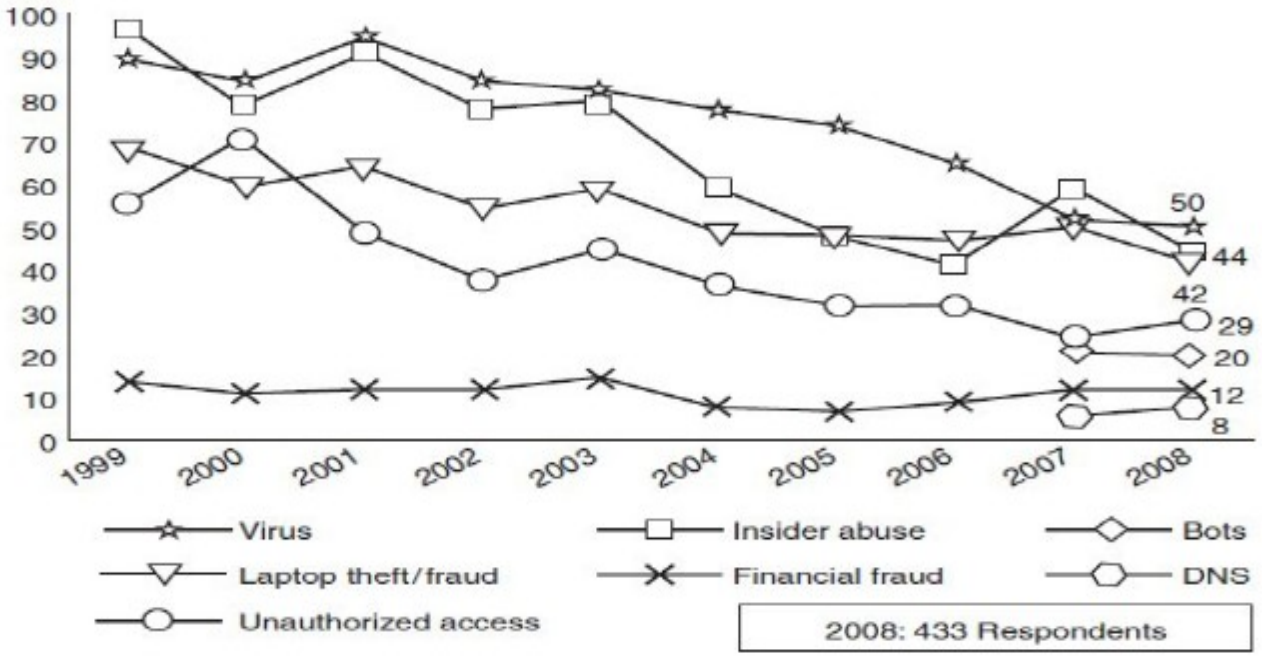


Figure 1.4 | Major types of incidents by percentage.
Source: 2008 CSI Computer Crime and Security Survey available at the link http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

COMPLAINTS BY AGGRIEVED WOMEN

Categories	2020-21	2019-20
Cyber crime against women	797	458
Harassment of married women/ dowry harassment	4,209	3,963
Domestic violence	6,049	3,369
Right to live with dignity	8,688	5,061
Police apathy	1,460	1,968

Source: www.newindianexpress.com

- Typical network misuses are
  - Internet radio/streaming audio,
  - streaming video,
  - file sharing,
  - instant messaging,
  - online gaming,
  - Online gambling is illegal in some countries – for example, in India.

- A Botnet maker can control the group remotely for illegal purposes, the most common being
  - denial-of-service attack (DoS attack),
  - Adware,
  - Spyware,
  - E-Mail Spam,
  - Click Fraud
  - theft of application serial numbers,
  - login IDs
- financial information such as credit card numbers, etc.

- An attacker usually gains control by infecting the computers with a virus or other Malicious Code. The computer may continue to operate normally without the owner's knowledge that his computer has been compromised.

- The problem of Botnet is global in nature and India is also facing the same.

- India has an average of 374 new Bot attacks per day and had more than 38,000 distinct Bot-infected computers in the first half of the year 2009.

- Small and medium businesses in the country are at greater risk, as they are highly vulnerable to Bots, Phishing, Spam and Malicious Code attacks.
  - Mumbai with 33% incidences tops the Bot-infected city list,
  - followed by New Delhi at 25%,
  - Chennai at 17% and
  - Bangalore at 13%.

- Tier-II locations are now also a target of Bot-networks with Bhopal at 4% and Hyderabad, Surat, Pune and Noida at 1% each.

- The Internet is a network of interconnected computers. *If the computers, computer systems, computer resources, etc. are unsecured and vulnerable to security threats, it can be detrimental to the critical infrastructure of the country.*

Box 1.2 | The Botnet Menace!

- **Botnet: A** group of computers that are controlled by software containing harmful programs, without their users' knowledge
- The term "Botnet" is used to refer to a group of compromised computers (*zombie computers, i.e., personal computers secretly under the control of hackers*) running malwares under a common command and control infrastructure. Figure 1.3 shows how a "zombie" works.

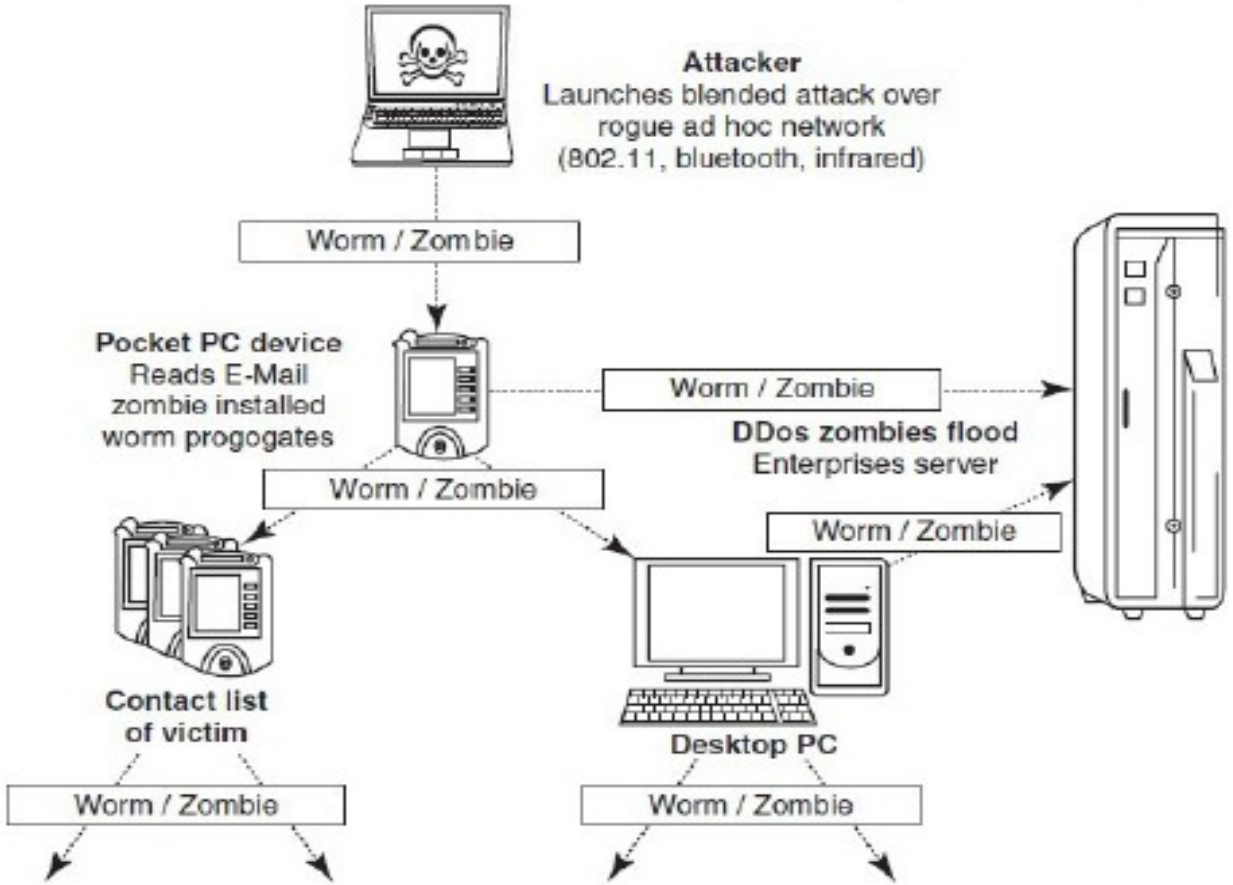


Figure 1.3 | How a zombie works.

1.4 Who are Cybercriminals?

- Cybercriminals are those who conduct acts such as:
  - Child pornography
  - Credit card fraud
  - Cyberstalking
  - Defaming another online
  - Gaining unauthorized access to computer systems
  - Ignoring copyrights
  - Software licensing and trademark protection
  - Overriding encryption to make illegal copies
  - Software piracy
  - Stealing another's identity to perform criminal acts

Categorization of Cybercriminals

- Type 1: Cybercriminals- hungry for recognition
  - Hobby hackers
    - A person who enjoys exploring the limits of what is possible, in a spirit of playful cleverness. May modify hardware/ software.
  - IT professional(social engineering):
    - Ethical hacker
  - Politically motivated hackers :
    - promotes the objectives of individuals, groups or nations supporting a variety of causes such as : Anti globalization, transnational conflicts and protest.
  - Terrorist organizations
    - Cyberterrorism.
    - Use the internet attacks in terrorist activity.
    - Large scale disruption of computer networks, personal computers attached to internet via viruses.

Categorization of Cybercriminals

Type 2: Cybercriminals- not interested in recognition

- Psychological perverts
  - Express sexual desires, deviates from normal behaviour
- Financially motivated hackers
  - Make money from cyber attacks
  - Bots-for-hire : fraud through phishing, information theft, spam and extortion
- State-sponsored hacking
  - Hacktivists
  - Extremely professional groups working for governments
  - Have ability to worm into the networks of the media, major corporations, defence departments

Categorization of Cybercriminals

Type 3: Cybercriminals- the insiders

- Disgruntled or former employees seeking revenge
- Competing companies using employees to gain economic advantage through damage and/ or theft.

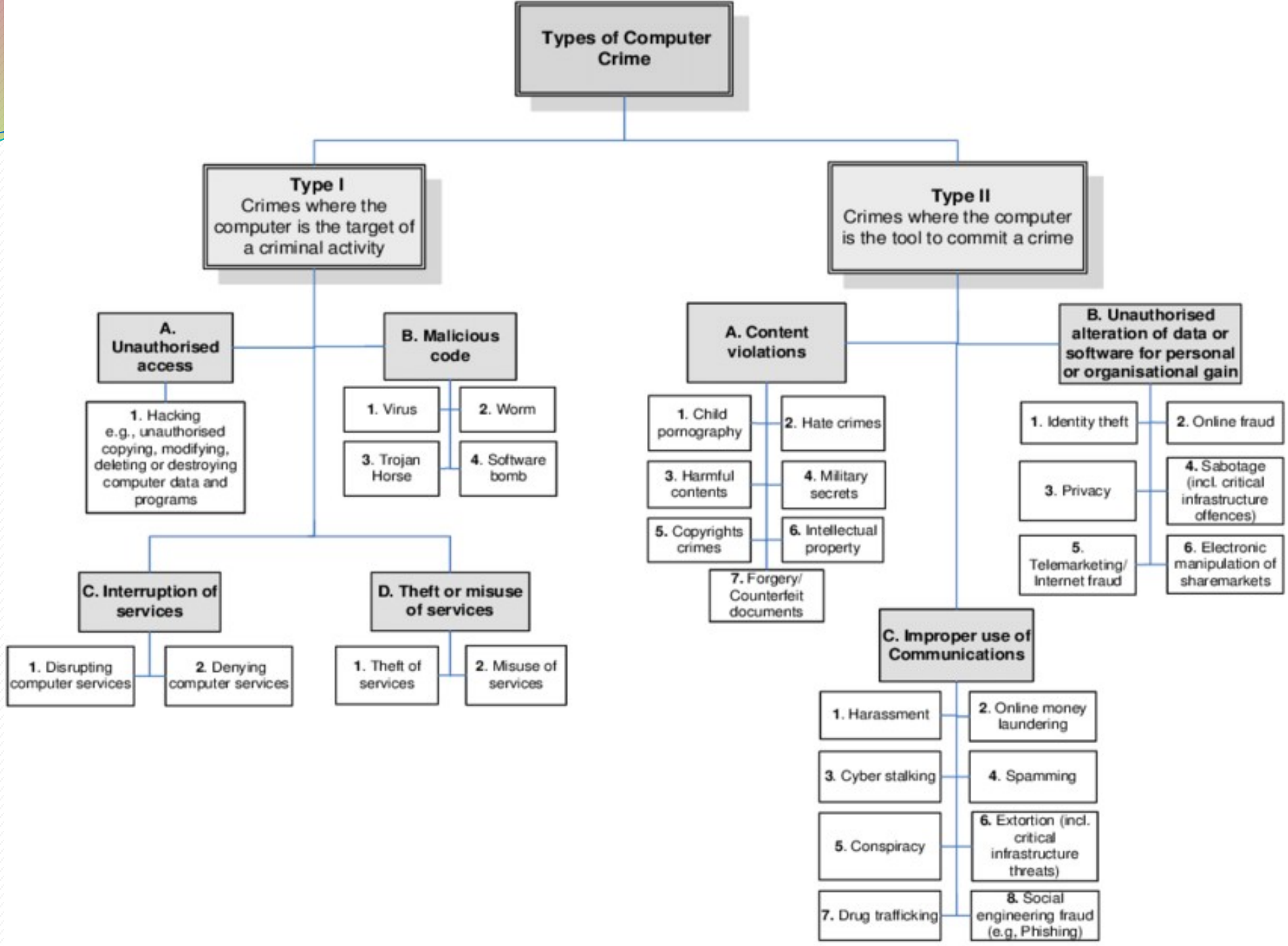
- "Crime is defined as "an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the off ender liable to punishment by that law"

Classification of Cybercrimes

Table 1.6 | Classifying cybercrimes – broad and narrow

	Cybercrime in Narrow Sense	*Cybercrime in Broad Sense*	
Role of computer	*Computer as an object* The computer/information stored on the computer is the subject/target of the crime	*Computer as a tool* The computer/or information stored on the computer constitutes an important tool for committing the crime	*Computer as the environment or context* The computer/information stored on the computer plays a non-substantial role in the act of crime, but does contain evidence of the crime
Examples	Hacking, computer sabotage, DDoS-attacks (distributed denial-of-service attacks), virtual child pornography	Computer fraud, forgery distribution of child pornography	Murder using computer techniques, bank robbery and drugs trade

Table 1.6 presents a scheme for cybercrime classification (broad and narrow classification).


Types of Computer Crime
Type I
Crimes where the computer is the target of a criminal activity
Type II
Crimes where the computer is the tool to commit a crime
A. Unauthorised access
1. Hacking e.g., unauthorised copying, modifying, deleting or destroying computer data and programs
B. Malicious code
1. Virus
2. Worm
3. Trojan Horse
4. Software bomb
C. Interruption of services
1. Disrupting computer services
2. Denying computer services
D. Theft or misuse of services
1. Theft of services
2. Misuse of services
A. Content violations
1. Child pornography
2. Hate crimes
3. Harmful contents
4. Military secrets
5. Copyrights crimes
6. Intellectual property
7. Forgery/ Counterfeit documents
B. Unauthorised alteration of data or software for personal or organisational gain
1. Identity theft
2. Online fraud
3. Privacy
4. Sabotage (incl. critical infrastructure offences)
5. Telemarketing/ Internet fraud
6. Electronic manipulation of sharemarkets
C. Improper use of Communications
1. Harassment
2. Online money laundering
3. Cyber stalking
4. Spamming
5. Conspiracy
6. Extortion (incl. critical infrastructure threats)
7. Drug trafficking
8. Social engineering fraud (e.g. Phishing)

Motives behind cybercrime

- Greed
- Desire to gain power
- Publicity
- Desire for revenge
- A sense of adventure
- Looking for thrill to access forbidden information
- Destructive mindset
- Desire to sell network security services

1.5 Classification of cybercrimes

1. Cybercrime against an individual
2. Cybercrime against property
3. Cybercrime against organization
4. Cybercrime against Society
5. Crimes emanating from Usenet newsgroup

1. Cybercrime against an individual

- Electronic mail spoofing and other online frauds
- Phishing, spear phishing
- Spamming
- Cyber-defamation
- Cyberstalking and harassment
- Computer sabotage
- Pornographic offences
- Password-sniffing

1. Cybercrime against an individual

- Electronic mail (E-Mail) Spoofing and other online frauds :
- A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source.
- For example, let us say, Roopa has an E-Mail address roopa@asianlaws.org.
- Let us say her boyfriend Suresh and she happen to have a show down. Then Suresh, having become her enemy, spoofs her E-Mail and sends vulgar messages to all her acquaintances.
- Since the E-Mails appear to have originated from Roopa, her friends could take offence and relationships could be spoiled for life.

1. Cybercrime against an individual

- E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.
- To send spoofed e-mail, senders insert commands in headers that will alter message information.
- It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say.
- Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write.
- Classic examples of senders who might prefer to disguise the source of the e-mail include a sender reporting mistreatment by a spouse to a welfare agency.

1. Cybercrime against an individual

- Although most spoofed e-mail falls into the "nuisance" category and requires little action other than deletion, the more malicious varieties can cause serious problems and security risks.
- For example, spoofed e-mail may purport to be from someone in a position of authority, asking for sensitive data, such as passwords, credit card numbers, or other personal information -- any of which can be used for a variety of criminal purposes.
- The Bank of America, eBay, and Wells Fargo are among the companies recently spoofed in mass spam mailings.
- *One type of e-mail spoofing, self-sending spam, involves messages that appear to be both to and from the recipient.*

Email Spoofing cases:

- https://indianexpress.com/article/cities/mumbai/using-e-mail-spoofing-fraudster-dupes-bank-of-rs-9-94-lakh-7429133/#:~:text=In%20a%20case%20of%20cyber,a%20fake%20email%20id%2C%20which
- https://timesofindia.indiatimes.com/city/mumbai/paint-giant-loses-rs-28-lakh-in-case-of-email-spoofing/articleshow/67580796.cms
- https://timesofindia.indiatimes.com/city/pune/crooks-use-email-spoofing-to-cheat-firm-of-rs-27-8-lakh/articleshow/80522115.cms

1. Cybercrime against an individual

- Online Frauds
- Online Scams. There are a few major types of crimes under the category of hacking:
- Spoofing website and E-Mail security alerts , false mails about virus threats, lottery frauds and Spoofing. In Spoofing websites and E-Mail security threats, fraudsters create authentic looking websites that are actually nothing but a spoof.
- The purpose of these websites is to make the user enter personal information which is then used to access business and bank accounts.
- Fraudsters are increasingly turning to E-Mail to generate traffic to these websites.
- This kind of online fraud is common in banking and financial sector.
- There is a rise in the number of financial institutions' customers who receive such Emails which usually contain a link to a spoof website.

1. Cybercrime against an individual

- Online Frauds
- It may mislead users to enter user ids and passwords on the pretence that security details can be updated or passwords changed.
- It is wise to be alert and careful about E-Mails containing an embedded link, with a request for you to enter secret details. It is strongly recommended not to input any sensitive information that might help criminals to gain access to sensitive information, such as bank account details, even if the page appears legitimate.
- In virus E-Mails, the warnings may be genuine, so there is always a dilemma whether to take them lightly or seriously.
- A wise action is to first confirm by visiting an antivirus site such as McAfee, Sophos or Symantec before taking any action, such as forwarding them to friends and colleagues.

1. Cybercrime against an individual

- Phishing, Spear Phishing and its various other forms such as Vishing and Smishing
- "**Phishing**" refers to an attack using mail programs to deceive or coax (lure) Internet users into disclosing confidential information that can be then exploited for illegal purposes.
- "**Spear Phishing**" is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering.
- Here "**Vishing**" is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward.
- The term is a combination of V – voice and Phishing
- Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.

1. Cybercrime against an individual

- Phishing, Spear Phishing and its various other forms such as Vishing and Smishing
- The most profitable uses of the information gained through a Vishing attack include:
- **1.** ID theft;
- **2.** purchasing luxury goods and services;
- **3.** transferring money/funds;
- **4.** monitoring the victims' bank accounts;
- **5.** making applications for loans and credit cards.
- "Smishing" is a criminal offence conducted by using social engineering techniques similar to Phishing.
- The name is derived from "SMS Phishing" SMS – Short Message Service – is the text messages communication component dominantly used into mobile phones.

1. Cybercrime against an individual

- Spamming:
- People who create electronic Spam are called spammers.
- Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unrequested bulk messages indiscriminately.
- Although the most widely recognized form of Spam is E-Mail Spam, the term is applied to similar abuses in other media:

Recent Phishing case:
https://www.indiatoday.in/coronavirus-outbreak/story/phishing-cases-rise-cyber-frauds-covid-testing-booster-doses-1896936-2022-01-06

1. Cybercrime against an individual

- Instant messaging Spam,
- Usenet newsgroup Spam,
- Web search engine Spam,
- Spam in blogs,
- Wiki Spam,
- Online classified ads Spam,
- Mobile phone messaging Spam,
- Internet forum Spam,
- Junk fax transmissions,
- Social networking Spam,
- File sharing network Spam,
- Video sharing sites, etc.

1. Cybercrime against an individual

- Spamming is difficult to control because it has economic inability – advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings.
- Spammers are numerous; the volume of unrequested mail has become very high because the barrier to entry is low.
- The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers (ISPs), who are forced to add extra capacity to cope with the deluge.
- Spamming is widely detested, and has been the subject of legislation in many jurisdictions – for example, the CAN-SPAM Act of 2003.

1. Cybercrime against an individual

- *The **Controlling the Assault of Non-Solicited Pornography And Marketing** Act of 2003 is a law passed in 2003 establishing the United States' first national standards for the sending of commercial e-mail.*

1. Cybercrime against an individual

- Therefore, the following web publishing techniques should be avoided:
- 1. Repeating keywords.
- 2. Use of keywords that do not relate to the content on the site.
- 3. Use of fast meta refresh (a method of instructing a web browser to automatically refresh the current web page or frame after a given time interval).
- 4. Redirection (the process of forwarding one URL to a different URL).
- 5. IP Cloaking (the masking of the sender's name and IP address in an e-mail note or distribution.)

1. Cybercrime against an individual

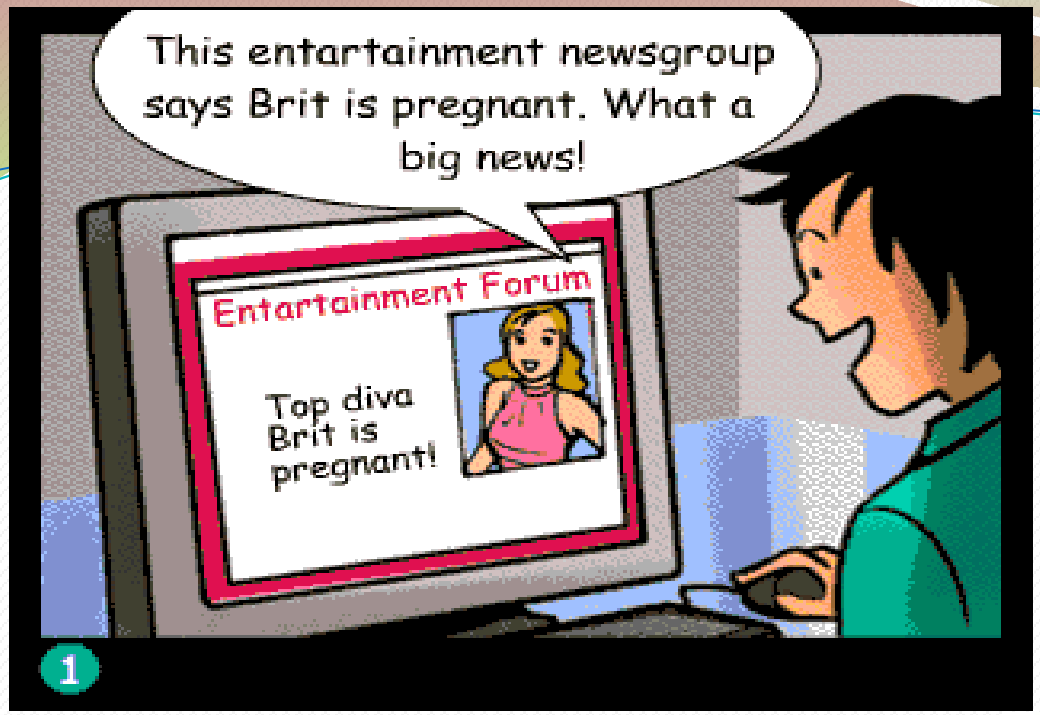
- 6. Use of coloured text on the same colour background.
- 7. Tiny text usage (adding to a page a text possibly as small as possible (usually 8px or even less) loaded with keywords).
- 8. Duplication of pages with different URLs.
- 9. Hidden links (Links whose font colours are the same as the background of a website).
- 10. Use of different pages that bridge to the same URL (gateway pages).

1. Cybercrime against an individual

- Search engine spamming
- Alteration or creation of a document with the intent to deceive an electronic catalogue or a filing system
- Some web authors use “subversive techniques” to ensure that their site appears more frequently or higher number in returned search results.
- Remedy: permanently exclude from the search index

1. Cybercrime against an individual

- Cyber defamation:
- Cyber defamation is a Software offence
- Let us first understand what the term entails. CHAPTER XXI of the Indian Penal Code (IPC) is about DEFAMATION.
- In Section 499 of CHAPTER XXI of IPC, regarding “defamation” there is a mention that “Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, **or**
- Knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.”


This entartainment newsgroup says Brit is pregnant. What a big news!
Entartainment Forum
Top diva Brit is pregnant!
1


Hey, I read on wikipedia that your mom —
Funny, 'cause the version I read had your mom's photo.

1. Cybercrime against an individual

- Cyber-defamation happens when the above takes place in an electronic form.
- In other words, “cyber-defamation” occurs when defamation takes place with the help of computers and/or the Internet.
- For example, someone publishes defamatory matter about someone on a website or sends an E-Mail containing defamatory information to all friends of that person.

1. Cybercrime against an individual

- According to the IPC Section 499:
- 1. It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.
- An imputation is made concerning a company or an association or collection of people as such.
- 2. An imputation in the form of an alternative or expressed ironically
- 3. An imputation that directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, **or**
- lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person.

1. Cybercrime against an individual

Types of defamation

- Libel : Written defamation
- Slander: Oral defamation
- The plaintiff must have to show that the defamatory statements were unlawful and would indeed injure the person's or organization's reputation.
- When failed to prove, the person who made the allegations may still be held responsible for defamation.

Some cyber defamation cases in India:
https://indiankanoon.org/search/?formInput=cyber+defamation-+indian+cases

1. Cybercrime against an individual

Cyber defamation cases

- In first case of cyber defamation in India (14 Dec 2009),
  - the employee of a corporate defamed its reputation was sending derogatory and defamatory emails against the company and its managing director
  - In this case the Court(Delhi court) had restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails.
  - The court passed as important ex-parte injunction.
- In another case, accused posted obscene, defamatory and annoying message about a divorcee woman and also sent emails to the victim.
  - The offender was traced and was held guilty of offences under section 469, 509 IPC and 67 of IT Act, 2000.
- Other defamation cases:
  - A malicious customer review by a competitor could destroy a small business.
  - A false accusation of adultery on a social networking site could destroy a marriage.
  - An allegation that someone is a “crook” could be read by a potential employer or business partner

1. Cybercrime against an individual

- Cyberstalking and Harassment :
- The dictionary meaning of “stalking” is an “act or process of following prey stealthily – trying to approach somebody or something.”
- Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- The behaviour includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.

1. Cybercrime against an individual

- Cyberstalking and Harassment :
- Cyberstalking cases:
- https://blog.ipleaders.in/virtual-reality-cyberstalking-india/#:~:text=Maharashtra%20was%20also%20responsible%20for,by%20Haryana%20with%2097%20case
- https://www.legalserviceindia.com/legal/article-1048-cyber-stalking-in-india.html
- https://indiankanoon.org/search/?formInput=cyber+stalking+and+harassment+cases

1. Cybercrime against an individual

- Computer Sabotage:
- The use of the Internet to stop the normal functioning of a computer system through the introduction of worms, viruses or logic bombs, is referred to as computer sabotage.
- It can be used to gain economic advantage over a competitor, to promote the illegal activities of terrorists or to steal data or programs for extortion purposes.
- Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs.
- Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date

1. Cybercrime against an individual

- Pornographic Offences:
- “Child pornography” means any visual depiction, including but not limited to the following:
- 1. Any photograph that can be considered obscene and/or unsuitable for the age of child viewer;
- 2. film, video, picture;
- 3. computer-generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

1. Cybercrime against an individual

- Pornographic Offences:
- The Internet has become a household commodity in the urban areas of the nation. Its explosion has made the children a viable victim to the cybercrime .
- As the broad-band connections get into the reach of more and more homes, larger child population will be using the Internet and therefore greater would be the chances of falling victim to the aggression of pedophiles.
- “Pedophiles” a person who is sexually attracted to children.
- Following steps show how pedophiles operate:

1. Cybercrime against an individual

- Pornographic Offences:
- Step 1: Paedophiles use a false identity to trap the children/teenagers (using “false identity” which in itself is another crime called “identity theft”).
- Step 2: They seek children/teens in the kids’ areas on the services, such as the Games BB or chat areas where the children gather .
- Step 3: They befriend children/teens.
- Step 4: They extract personal information from the child/teen by winning his/her confidence.
- Step 5: Pedophiles get E-Mail address of the child/teen and start making contacts on the victim’s E-Mail address as well.
- Sometimes, these E-Mails contain sexually explicit language.

1. Cybercrime against an individual

- Pornographic Offences:
- Step 6: They start sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his/her inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
- Step 7: At the end of it, the pedophiles set up a meeting with the child/teen out of the house and then drag him/her into the net to further sexually assault him/her or to use him/her as a sex object.
- This is the “digital world”; in physical world, parents know the face of dangers and they know how to avoid and face the problems by following simple rules and accordingly they advice their children to keep away from dangerous things and ways.

1. Cybercrime against an individual

- Pornographic Offences:
- However, it is possible, even in the modern times most parents may not know the basics of the Internet and the associated (hidden) dangers from the services offered over the Internet.
- Hence most children may remain unprotected in the cyber world.
- Paedophiles take advantage of this situation and lure the children, who are not advised by their parents or by their teachers about what is right/wrong for them while browsing the Internet.
- Legal remedies exist only to some extent;
  - For example, **Children's Online Privacy Protection Act or COPPA** is a way of preventing online pornography.
  - COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

1. Cybercrime against an individual

- Password Sniffing:
- This also belongs to the category of cybercrimes against organization because the use of password could be by an individual for his/her personal work or the work he/she is doing using a computer that belongs to an organization.

- Case study
- https://inc42.com/buzz/1-4-lakh-upi-frauds-reported-in-q1-q2-2022-mha/

- https://indiankanoon.org/search/?formInput=credit%20card%20frauds+fromdate:1-1-2022+todate:31-12-2022

2.Cybercrime against property

- Credit Card Frauds:
- Information security requirements for anyone handling credit cards have been increased dramatically recently.
- Millions of dollars may be lost annually by consumers who have credit card and calling card numbers stolen from online databases.
- Security measures are improving, and traditional methods of law enforcement seem to be sufficient for prosecuting the thieves of such information.
- Bulletin boards and other online services are frequent targets for hackers who want to access large databases of credit card information.
- Security of cardholder data has become one of the biggest issues facing the payment card industry.

2.Cybercrime against property

- Payment Card Industry Data Security Standard (PCI-DSS) is a set of regulations developed jointly by the leading card schemes to prevent cardholder data theft and to help combat credit card fraud.
- PCI-DSS is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

2.Cybercrime against property

- Intellectual property(IP) crimes
- Basically, IP crimes include:
  - software piracy,
  - copyright infringement,
  - trademarks violations,
  - theft of computer source code, etc.

- Case Study
- https://www.intepat.com/blog/5-landmark-trademark-infringement-cases-2022/

- https://vakilsearch.com/blog/copyright-infringement-cases-in-india/
- https://indiankanoon.org/search/?formInput=ipr%20cases

2.Cybercrime against property

- Internet Time Theft
- Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person.
- Basically, Internet time theft comes under hacking because the person who gets access to someone else's ISP 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 .
- However, one can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent.
- The issue of Internet time theft is related to the crimes conducted through "identity theft."

3.Cybercrime against organization

- Unauthorized accessing of computer :
- Hacking is one method of doing this and hacking is a punishable offence
- Password Sniffing :
- Password Sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site.
- Whoever installs the Sniffer can then impersonate an authorized user and login to access restricted documents.
- Laws are not yet set up to adequately prosecute a person for impersonating another person online.
- Laws designed to prevent unauthorized access to information may be effective in apprehending crackers using Sniffer programs.

3.Cybercrime against organization

- Denial-of-Service attacks (known as DoS attacks):
- The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it.
- A DoS attack may do the following:
- 1. Flood a network with traffic, thereby preventing legitimate network traffic.
- 2. Disrupt connections between two systems, thereby preventing access to a service.
- 3. Prevent a particular individual from accessing a service.
- 4. Disrupt service to a specific system or person.

3.Cybercrime against organization

- Virus attacks:
- Virus attacks can be used to damage the system to make the system unavailable
- Computer virus is a program that can “infect” legitimate (valid) programs by modifying them to include a possibly “evolved” copy of itself.
- Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.
- A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person.
- Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern.
- Viruses can often spread without any readily visible symptoms.

3.Cybercrime against organization

- E-Mail Bombing/Mail bombs:
- E-Mail bombing refers to sending a large number of E-Mails to the victim to crash victim's E-Mail account (in the case of an individual) or
- to make victim's mail servers crash (in the case of a company or an E-Mail service provider).
- Computer program can be written to instruct a computer to do such tasks on a repeated basis.
- In recent times, terrorism has hit the Internet in the form of mail bombings.
- By instructing a computer to repeatedly send E-Mail to a specified person's E-Mail address, the cybercriminal can overwhelm the recipient's personal account and potentially shut down entire systems.
- This may or may not be illegal, but it is certainly disruptive.

3.Cybercrime against organization

- Salami attack/Salami technique:
- These attacks are used for committing financial crimes.
- A salami attack is a series of smaller attacks that together result in a large-scale attack.
- The idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed;
- For example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say ` 2/- or a few cents in a month) from the account of every customer.
- No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month.

3.Cybercrime against organization

- Logic bomb
- A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.
- Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs.
- Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.
- For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company.

3.Cybercrime against organization

- Trojan Horse:
- Trojan Horses: A Trojan Horse, Trojan for short, is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.
- For example, The victim receives an official-looking email with an attachment. The attachment contains malicious code that is executed as soon as the victim clicks on the attachment.
- Data Diddling:
- A data diddling (data cheating) attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.
- E.g. Electricity Boards in India have been victims to data diddling programs inserted when private parties computerize their systems.

3.Cybercrime against organization

- Industrial Spying/Industrial Espionage:
- Spying is not limited to governments. Corporations, like governments, often spy on the enemy.
- The Internet and privately networked systems provide new and better opportunities for espionage.
- “Spies” can get information about product finances , research and development and marketing strategies, an activity known as “industrial spying”.
- However, cyber-spies rarely leave behind a trail.

3.Cybercrime against organization

- Industrial Spying/Industrial Espionage:
- Industrial spying is not new; in fact it is as old as industries themselves. The use of the Internet to achieve this is probably as old as the Internet itself.
- Traditionally, this has been the reserved hunting field of a few hundreds of highly skilled hackers, contracted by high-profile companies or certain governments via the means of registered organizations (it is said that they get several hundreds of thousands of dollars, depending on the “assignment”).
- With the growing public availability of Trojans and Spyware material, even low-skilled individuals are now inclined to generate high volume profit out of industrial spying.
- This is referred to as “Targeted Attacks” (which includes “Spear Phishing”).

3.Cybercrime against organization

- Example of Industrial Espionage
- A Chinese Trojan horse email campaign targeted some 140 senior Israeli defence corporation employees (2013) involved in highly classified, sensitive security projects.
- The email was made to appear as if it came from a known German company that regularly works with the Israeli defence industry.
- However, it turned out to contain a Trojan horse, which, according to the report, attempted to funnel information from the recipients' computers.
- The Trojan horse was noticed by computer defence systems and shutdown.
- The defence establishment then realized how many Israelis received the email, and reportedly tracked the malicious program down to Chinese defence industries.
- The incident led security companies to reiterate to employees computer security guidelines.
- https://www.timesofisrael.com/israel-reportedly-thwarts-cyber-attack-from-china/

3.Cybercrime against organization

- Computer Network Intrusions:
- Crackers “who are often misnamed” Hackers can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert Trojan Horses or change user names and passwords.
- Network intrusions are illegal, but detection and enforcement are difficult.
- Current laws are limited and many intrusions go undetected.
- The cracker can bypass existing password protection by creating a program to capture logon IDs and passwords.
- The practice of “strong password” is therefore important.

3.Cybercrime against organization

- Software Piracy :
- This is a big challenge area indeed.
- Cybercrime investigation cell of India defines “software piracy” as theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.
- There are many examples of software piracy:
  - end-user copying – friends loaning disks to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses;
  - hard disk loading with illicit means – hard disk vendors load pirated software;
  - counterfeiting – large-scale duplication and distribution of illegally copied software;

3.Cybercrime against organization

- Software Piracy :
  - illegal downloads from the Internet – by intrusion, by cracking serial numbers, etc. Beware that those who buy pirated software have a lot to lose:
  - (a) getting untested software that may have been copied thousands of times over,
  - (b) the software, if pirated, may potentially contain hard-drive-infecting viruses,
  - (c) there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users,
  - (d) there is no warranty protection,
  - (e) there is no legal right to use the product, etc.

4.Cybercrime against Society

- Forgery
- Counterfeit currency notes, postage and revenue stamps, mark sheets, etc. can be forged using sophisticated computers, printers and scanners.
- Outside many colleges there are miscreants soliciting the sale of fake mark-sheets or even degree certificates.
- These are made using computers and high quality scanners and printers.
- In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.

4.Cybercrime against Society

- Forgery
- Stamp Paper Scam – a racket that flourished on loopholes in the system
- Abdul Karim Telgi, the mastermind of the multi-crore counterfeiting, printed fake stamp papers worth thousands of crores of rupees using printing machines purchased illegally with the help of some conniving officials of the Central Govt.'s Security Printing Press (India Security Press) located in Nashik.
- These fake stamp papers penetrated in more than 12 states through a widespread network of vendors who sold the counterfeits without any fear and earned hefty commissions.
- Amount swindled Rs. 172 crores
- Telgi is in jail serving his 13 plus 10 years term

- https://blog.ipleaders.in/telgi-scam/

4.Cybercrime against Society

- Cyberterrorism:
- Cyberterrorism is defined as “any person, group or organization who, with terrorist intent, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyber terrorism.”
- https://journals.indexcopernicus.com/api/file/viewByFileId/783266.pdf

- Web Jacking:
- Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it).
- Thus, the first stage of this crime involves “password sniffing.”
- The actual owner of the website does not have any more control over what appears on that website.

4.Cybercrime against Society

- Web Jacking:
- Recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein.
- Further the site of Bombay crime branch was also web jacked.
- Another case of web jacking is that of the 'gold fish' case. In this case the site was hacked and the information pertaining to gold fish was changed.

5.Crimes emanating from Usenet newsgroup

- By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive in another way.
- Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk.
- Usenet is a popular means of sharing and distributing information on the Web with respect to specific topic or subjects.
- Usenet is a mechanism that allows sharing information in a many-to-many manner.
- The newsgroups are spread across 30,000 different topics.
- In principle, it is possible to prevent the distribution of specific newsgroup.

- **UseNet - > USEr NETwork**

5.Crimes emanating from Usenet newsgroup

- In reality, however, there is no technical method available for controlling the contents of any newsgroup.
- It is merely subject to self-regulation and net etiquette.
- It is feasible to block specific newsgroups, however, this cannot be considered as a definitive solution to illegal or harmful content.
- It is possible to put Usenet to following criminal use:
  - 1. Distribution/sale of pornographic material;
  - 2. distribution/sale of pirated software packages;
  - 3. distribution of hacking software;
  - 4. sale of stolen credit card numbers.
  - 5. sale of stolen data/stolen property.

5.Crimes emanating from Usenet newsgroup

- Usenet were largely replaced by web-based discussion groups and chat tools such as ICQ (I Seek You) and IRC (Internet Relay Chat utility).
- ICQ is an Internet tool that notifies you when other users are online and enables you to communicate with them. ICQ works much like an instant messenger.
- With an IRC, you can connect to a remote server where other users are also connected and talk with them.
- In recent time communication/chat applications such as WhatsApp, Telegram, Skype, Signal, etc. have replaced these applications as well.

- https://www.techspot.com/article/1771-icq/

Biggest Cyber Breaches in India

https://www.policybazaar.com/corporate-insurance/articles/biggest-cyber-breaches-in-india/#:~:text=Air%20India%20Cyber%20Breach%20(May%202021

CYBER OFFENCES

How Criminals Plan Them? - Introduction

- Technology is a “double-edged sword” as it can be used for both good and bad purposes.
- People with the tendency to cause damages or carrying out illegal activities will use it for bad purpose.
- Computers and tools available in IT are also used as either target of offence
- In today’s world of Internet and computer networks, a criminal activity can be carried out across national borders.
- Chapter 1 provided an overview of the most commonly occurring crimes that target the computer.
- Cybercriminal use the World Wide Web and Internet to an optimum level for all illegal activities to store data, contacts, account information, etc.
- The criminals take advantage of the lack of awareness about cybercrimes and cyberlaws among the people who are constantly using the IT infrastructure for official and personal purposes.
- People who commit cybercrimes are known as “Crackers” (Box 2.1).

Box 2.1 | Hackers, Crackers and Phreakers

Hacker: A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them. Hackers are usually very talented, smart people who understand computers better than others. The term is often confused with cracker that defines someone who breaks into computers (refer to Box 2.2).

Brute Force hacking: A technique used to find passwords or encryption keys by trying every possible combination of letters, numbers, etc., until the code is broken.

Cracker: A cracker is a person who breaks into computers. Crackers should not be confused with hackers. The term “cracker” is usually connected to computer criminals. Some of their crimes include vandalism, theft and snooping in unauthorized areas.

Cracking: It is the act of breaking into computers. Cracking is a popular, growing subject on the Internet. Many sites are devoted to supplying crackers with programs that allow them to crack computer

Some of these programs contain dictionaries for guessing passwords. Others are used to break into phone lines (called “phreaking”). These sites usually display warnings such as “These fi les are illegal; we are not responsible for what you do with them.”

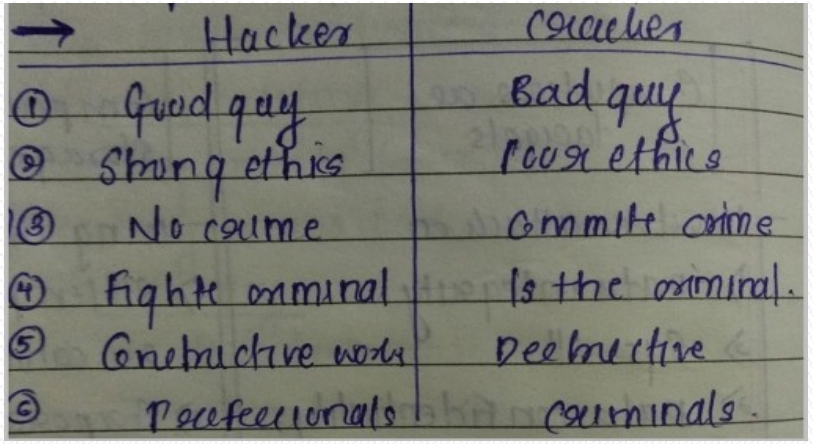
Cracker tools: These are programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Trojans, viruses, war diallers and worms.

Phreaking: This is the notorious art of breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.

War Dialler: It is program that automatically dials phone numbers looking for computers on the other end. It catalogues numbers so that the hackers can call back and try to break in.

How Criminals Plan Them? - Introduction

- An attacker would look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected.
- The categories of vulnerabilities that hackers typically search for are the following:
  1. Inadequate border protection (border as in the sense of network periphery);
  2. Remote access servers (RASs) with weak access controls;
  3. Application servers with well-known exploits;
  4. Misconfigured systems and systems with default configurations.
- To help the reader understand the network attack scenario, Fig. 2.2 illustrates a small network highlighting specific occurrences of several vulnerabilities described above.



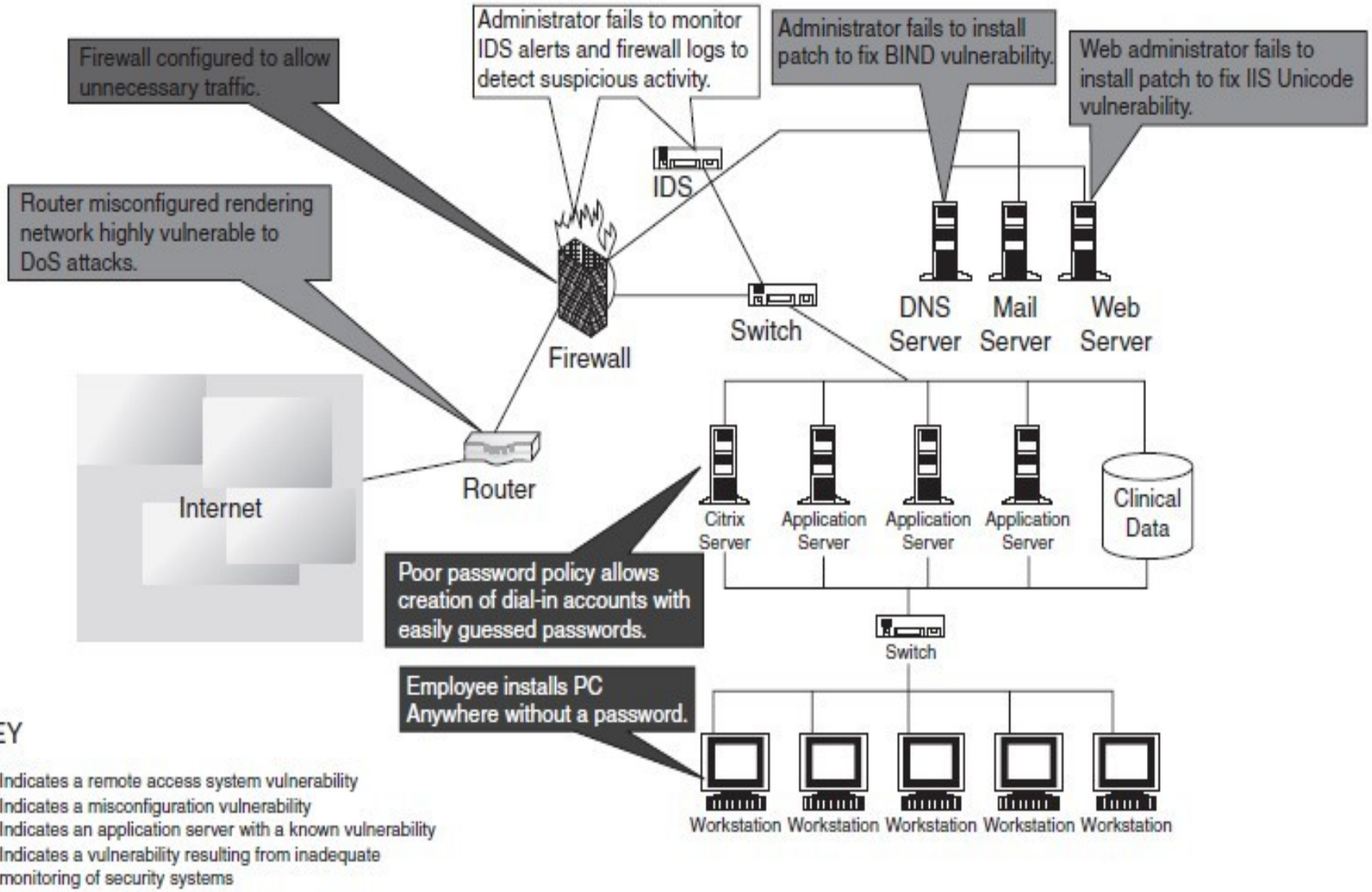


Figure 2.2 | Network vulnerabilities – sample network.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Fig. 11.6), Wiley India.

Box 2.2 | What Color is Your Hat in the Security World?

*A **black hat*** is also called a "cracker" or "dark side hacker." Such a person is a malicious or **criminal hacker**. Typically, the term "cracker" is used within the security industry.

However, the general public uses the term hacker to refer to the same thing. In computer terminology, the meaning of "hacker" can be much broader. The name comes from the opposite of "white hat hackers."

*A **white hat hacker*** is considered an ***ethical hacker***. In the realm of IT, a "white hat hacker" is a person who is ethically opposed to the abuse of computer systems.

It is said that the term is derived from American western movies, where the protagonist typically wore a white cowboy hat and the antagonist typically wore a black one.

As a simplified explanation, a "white hat" generally focuses on securing IT systems, whereas a "black hat" (the opposite) would like to break into them, so this sounds like an age-old game of a thief and a police.

*A **brown hat hacker*** is one who thinks before acting or committing a malice or non-malice deed.

A grey hat commonly refers to a hacker who releases information about any exploits or security holes he/she finds openly to the public. He/she does so without concern for how the information is used in the end (whether for patching or exploiting).

Categories of Cybercrime

- Cybercrime can be categorized based on the following:

1. The target of the crime and
2. whether the crime occurs as a single event or as a series of events.

- Cybercrime can be targeted against individuals (persons), assets (property) and/or
- organizations (government, business and social).

1. *Crimes targeted at individuals*: The goal is to exploit human weakness such as greed and naivety.

- These crimes include financial frauds, sale of non-existent or stolen items, child pornography (explained in Chapter 1), copyright violation, harassment, etc. with the development in the IT and the Internet; thus, criminals have a new tool that allows them to expand the pool of potential victims.
- However, this also makes difficult to trace and apprehend the criminals.

Categories of Cybercrime

2. *Crimes targeted at property*: This includes stealing mobile devices such as cell phone, laptops, personal digital assistant (PDAs), and removable media (CDs and pen drives); transmitting harmful programs that can disrupt functions of the systems and/or can wipe out data from hard disk, and can create the malfunctioning of the attached devices in the system such as modem, CD drive, etc.
3. *Crimes targeted at organizations*: Cyberterrorism is one of the distinct crimes against organizations/ governments.
   Attackers (individuals or groups of individuals) use computer tools and the Internet to usually terrorize the citizens of a particular country by stealing the private information, and also to damage the programs and files or plant programs to get control of the network and/or system (see Box 2.3).

Categories of Cybercrime

4. Single event of cybercrime: It is the single event from the perspective of the victim.
   For example, unknowingly open an attachment that may contain virus that will infect the system (PC/laptop). This is known as hacking or fraud.
5. Series of events: This involves attacker interacting with the victims repetitively.
   For example, attacker interacts with the victim on the phone and/ or via chat rooms to establish relationship first and then they exploit that relationship to commit the sexual assault.

Box 2.3 | Patriot Hacking

Patriot hacking[1] also known as ***Digital Warfare***, is a form of vigilante computer systems' cracking done by individuals or groups (usually citizens or supports of a country) against a real or perceived threat.

Traditionally, Western countries, that is, developing countries, attempts to launch attacks on their perceived enemies.

Although patriot hacking is declared as illegal in the US, however, it is reserved only for government agencies [i.e., Central Intelligence Agency (CIA) and National Security Agency (NSA)] as a legitimate form of attack and defense. Federal Bureau of Investigation (FBI) raised the concern about rise in cyberattacks like website defacements (explained in Box 1.4, Chapter 1) and denial-of-service attacks (DoS – refer to Section 4.9, Chapter 4), which adds as fuel into increase in international tension and gets mirrored it into the online world.

After the war in Iraq in 2003, it is getting popular in the North America, Western Europe and Israel. These are countries that have the greatest threat to Islamic terrorism and its aforementioned digital version.

The People's Republic of China is allegedly making attacks upon the computer networks of the US and the UK. Refer to Box 5.15 in Chapter 5. For detailed information visit www.patriothacking.com

How Criminals Plan Attacks?

- Criminals use many methods and tools to locate the vulnerabilities of their target.
- The target can be an individual and/or an organization.
- Criminals plan passive and active attacks
- Active attacks are usually used to alter the system (i.e., computer network) whereas passive attacks attempt to gain information about the target.
- Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to violation of confidentiality.

- The following phases are involved in planning cybercrime:

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

Reconnaissance

- The literal meaning of “Reconnaissance” is an act of finding something or somebody (especially to gain information about an enemy or potential enemy).
- In the world of “hacking,” reconnaissance phase begins with “Footprinting” – this is the preparation toward pre-attack phase, and involves accumulating data about the target’s environment and computer architecture to find ways to intrude into that environment.
- Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities.
- The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack.
- Thus, an attacker attempts to gather information in two phases: passive and active attacks. Let us understand these two phases.

Passive Attacks

- A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge.
- It can be as simple as watching a building to identify what time employees enter the building premises.
- However, it is usually done using Internet searches or by Googling (i.e., searching the required information with the help of search engine Google) an individual or company to gain information.

Passive Attacks

1. Google or Yahoo search: People search to locate information about employees.
2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
3. Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target.
4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

Passive Attacks

- Tools used during passive attacks
- Google Earth
- Internet Archive
- Professional Community
- People Search
- Domain Name Confirmation
- WHOIS
- Netslookup
- Dnsstuff
- Traceroute
- VisualRoute Trace
- eMailTrackerPro
- HTTrack
- Website Watcher
- Competitive Intelligence

Active Attacks

- An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase.
- It involves the risk of detection and is also called “Rattling the doorknobs” or “Active reconnaissance.”
- Active reconnaissance can provide confirmation to an attacker about security measures in place (e.g., whether the front door is locked?), but the process can also increase the chance of being caught or raise a suspicion.

Active Attacks

- Tools used during active attacks
- Arphound
- Arping
- Bing
- Bugtraq
- Dig
- DNStracer
- Dsniff
- Filesnarf
- FindSMB
- Fping
- Fragroute
- Fragtest
- Hackbot
- Hmap
- Hping
- httping

Active Attacks

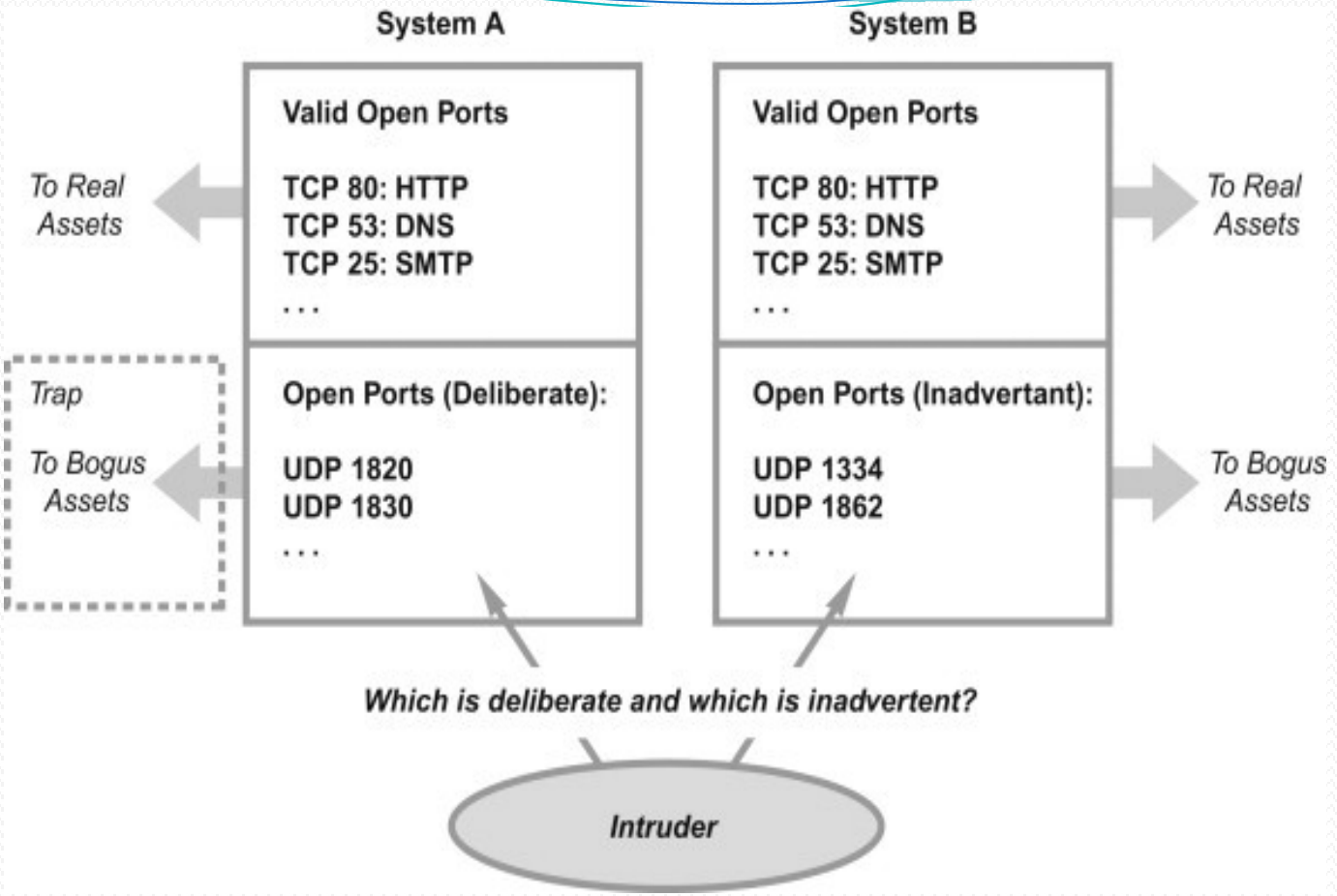
- Tools used during active attacks
- Hunt
- Libwhisker
- Mailsnarf
- Msgsnarf
- NBTScan
- Nessus
- Netcat
- Nikto
- Nmap
- Pathchar
- Ping
- scanSSH
- SMBclient
- SMTPScan
- TCPdump
- TCPreplay

Scanning and Scrutinizing Gathered Information

- Scanning is a key step to examine intelligently while gathering information about the target. The objectives of scanning are as follows:
- Port scanning: Identify open/close ports and services.
- Network scanning: Understand IP Addresses and related information about the computer network systems.
- Vulnerability scanning: Understand the existing weaknesses in the system.

How Port Scanner works?

The most popular port scanner is an open source tool called **nmap**.



A **port scanner** is an application designed to probe a server or host for open ports. Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.

Attack (Gaining and Maintaining the System Access)

- After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password.
2. exploit the privileges.
3. execute the malicious commands/applications.
4. hide the files (if required).
5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

Social Engineering

- Social engineering is the "technique to influence" and "persuasion to deceive" people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers' word, rather than exploiting computer security holes.
- It is generally agreed that people are the weak link in security and this principle makes social engineering possible.
- A social engineer usually uses telecommunication (i.e., telephone and/or cell phone) or Internet to get them to do something that is against the security practices and/or policies of the organization.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.

Social Engineering

- It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.
- The goal of a social engineer is to fool someone into providing valuable information or access to that information.
- Social engineer studies the human behavior so that people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting into trouble.
- The sign of truly successful social engineers is that they receive information without any suspicion.
- A simple example is calling a user and pretending to be someone from the service desk working on a network issue; the attacker then proceeds to ask questions about what the user is working on, what file shares he/she uses, what his/her password is, and so on…(see Box 2.6).

Box 2.6 | Social Engineering Example

Mr. Joshi: Hello?
The Caller: Hello, Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk space constraints on the file server, we will be moving few user's home directories to another disk. This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move and will be unavailable temporarily.

Mr. Joshi: Ohh … okay. I will be at my home by then, anyway.
Caller: Great!!! Please ensure to log off before you leave office. We just need to check a couple of things. What is your username?

Mr. Joshi: Username is "pjoshi." None of my files will be lost in the move, right?
Caller: No sir. But we will have to check your account to ensure the same. What is the password of that account?

Mr. Joshi: My password is "ABCD1965," all characters in upper case.
Caller: Ok, Mr. Joshi. Thank you for your cooperation. We will ensure that all the fi les are there.

Mr. Joshi: Thank you. Bye.
Caller: Bye and have a nice day.

Classification of Social Engineering

- Human-Based Social Engineering
- Human-based social engineering refers to person-to-person interaction to get the required/desired information.
- An example is calling the help desk and trying to find out a password.

1. Impersonating an employee or valid user:

- "Impersonation" is perhaps the greatest technique used by social engineers to deceive people.
- Social engineers "take advantage" of the fact that most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or
- to let someone into the building who "forgot" his/her badge, etc., or pretending to be an employee or valid user on the system.

Classification of Social Engineering

2. Posing as an important user:

- The attacker pretends to be an important user – for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system.
- The attacker uses intimidation so that a lower-level employee such as a help-desk worker will help him/her in gaining access to the system.
- Most of the low-level employees will not ask any question to someone who appears to be in a position of authority.

3. Using a third person:

- An attacker pretends to have permission from an authorized source to use a system.
- This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification

Classification of Social Engineering

4. Calling technical support:

- Calling the technical support for assistance is a classic social engineering example.
- Help-desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.

5. Shoulder surfing:

- It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.

Classification of Social Engineering

7. Dumpster diving:

- It involves looking in the trash for information written on pieces of paper or computer printouts.
- This is a typical North American term; it is used to describe the practice of rummaging through commercial or residential trash to find useful free items that have been discarded.
- It is also called dumpstering, binning, trashing, garbing or garbage gleaning.
- “Scavenging” is another term to describe these habits.
- In the UK, the practice is referred to as “ binning” or “skipping” and the person doing it is a “binner” or a “skipper.”

Computer-Based Social Engineering

- Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/ Internet.
- For example, sending a fake E-Mail to the user and asking him/her to re-enter a password in a webpage to confirm it.

1. Fake E-Mails:

- The attacker sends fake E-Mails (see Box 2.7) to users in such that the user finds it as a real e-mail.
- This activity is also called “Phishing”.
- It is an attempt to attract the Internet users (netizens) to reveal their personal information, such as usernames, passwords and credit card details by impersonating as a trustworthy and legitimate organization or an individual.
- Banks, financial institutes and payment gateways are the common targets.

Computer-Based Social Engineering

1. Fake E-Mails:

- Phishing is typically carried out through E-Mails or instant messaging and often directs users to enter details at a website, usually designed by the attacker with abiding the look and feel of the original website.
- Thus, Phishing is also an example of social engineering techniques used to fool netizens.
- The term "Phishing" has been evolved from the analogy that Internet scammers are using E-Mails attract to fish for passwords and financial data from the sea of Internet users (i.e., netizens).
- The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users.
- As hackers have a tendency of replacing "f" with "ph," the term "Phishing" came into being.

Computer-Based Social Engineering

2. E-Mail attachments:

- E-Mail attachments are used to send malicious code to a victim's system, which will automatically (e.g., keylogger utility to capture passwords) get executed.
- Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment.

3. Pop-up windows:

- Pop-up windows are also used, in a similar manner to E-Mail attachments.
- Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

Cyberstalking

- The dictionary meaning of “stalking” is an “act or process of following prey stealthily – trying to approach somebody or something.”
- Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- The behaviour includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.

Cyberstalking

- Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- It involves harassing or threatening behaviour that an individual will conduct repeatedly, for example, following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, **or**
- vandalizing against the person's property.
- As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

Types of Stalkers

- There are primarily two types of stalkers.

1. Online stalkers:

- They aim to start the interaction with the victim directly with the help of the Internet.
- E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone.
- The stalker makes sure that the victim recognizes the attack attempted on him/her.
- The stalker can make use of a third party to harass the victim.

Types of Stalkers

2. Offline stalkers:

- The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.
- Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet.
- The victim is not aware that the Internet has been used to perpetuate an attack against them.

Cases Reported on Cyberstalking

- The majority of cyberstalkers are men and the majority of their victims are women.
- Some cases also have been reported where women act as cyberstalkers and men as the victims as well as cases of same-sex cyberstalking.
- In many cases, the cyberstalker and the victim hold a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship, for example, ex-lover, ex-spouse, boss/subordinate, and neighbour.
- However, there also have been many instances of cyberstalking by strangers.

How Stalking Works?

- It is seen that stalking works in the following ways:

1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favours or threaten the victim.

How Stalking Works?

5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details (telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone nos), asking for sexual services or relationships.
7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails.

Case Study
• The Indian police have registered first case of cyberstalking in Delhi – the brief account of the case has been mentioned here. • To maintain confidentiality and privacy of the entities involved, we have changed their names.
• Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Bombay, and Ahmedabad.
• The said calls created havoc in the personal life destroying mental peace of Mrs. Joshi who decided to register a complaint with Delhi Police.
• A person was using her ID to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days.
• This person was chatting on the Internet, using her name and giving her address, talking in obscene language.
• The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.
• This was the first time when a case of cyberstalking was registered.
• Cyberstalking does not have a standard definition but it can be defined to mean threatening, unwarranted behavior, or advances directed by one person toward another person using Internet and other forms of online communication channels as medium.

Box 2.8 | Cyberbullying

- The National Crime Prevention Council defines Cyberbullying as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person."
- www.StopCyberbullying.org, an expert organization dedicated to Internet safety, security, and privacy defines cyberbullying as "a situation when a child, tween, or teen is repeatedly 'tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted' by another child, tween, or teen using text messaging, E-Mail, instant messaging, or any other type of digital technology."
- The practice of cyberbullying is not limited to children and, while the behavior is identified by the same definition in adults, the distinction in age groups is referred to as cyberstalking or cyberharassment when perpetrated by adults toward adults.[4]
- Source: http://en.wikipedia.org/wiki/Cyber-bullying (2 April 2009).

Cybercafé and Cybercrimes

- In February 2009, Nielsen survey on the profile of cybercafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15–35 years; 52% were graduates and postgraduates, though almost over 50% were students.
- Hence, it is extremely important to understand the IT security and governance practised in the cybercafes.
- In the past several years, many instances have been reported in India, where cybercafes are known to be used for either real or false terrorist communication.
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes.
- Cybercafes have also been used regularly for sending obscene mails to harass people.
- Public computers, usually referred to the systems, available in cybercafes, hold two types of risks.

Cybercafé and Cybercrimes

- First, we do not know what programs are installed on the computer – that is, risk of malicious programs such as keyloggers or Spyware, which maybe running at the background that can capture the keystrokes to know the passwords and other confidential information and/or monitor the browsing behaviour
- Second, over-the-shoulder surfing can enable others to find out your passwords. Therefore, one has to be extremely careful about protecting his/her privacy on such systems, as one does not know who will use the computer after him/her.

Cybercafé and Cybercrimes

- Indian Information Technology Act (ITA) 2000, does not define cybercafes and interprets cybercafes as “network service providers” referred to under the Section 79, which imposed on them a responsibility for “due diligence” failing which they would be liable for the offences committed in their network.
- Cybercriminals prefer cybercafes to carry out their activities.
- The criminals tend to identify one particular personal computer (PC) to prepare it for their use.
- Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target.
- Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week.

Cybercafé and Cybercrimes

- A recent survey conducted in one of the metropolitan cities in India reveals the following facts:

1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.
3. Several cybercafes had installed the software called "Deep Freeze" for protecting the computers from prospective malware attacks.
   Deep Freeze can wipe out the details of all activities carried out on the computer when one clicks on the "restart" button.

- Such practices present challenges to the police or crime investigators when they visit the cybercafes to pick up clues after the Interet Service Provider (ISP) points to a particular IP address from where a threat mail was probably sent or an online Phishing attack was carried out, to retrieve logged files.

Cybercafé and Cybercrimes

4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is down.
- Not having the AMC is a risk from cybercrime perspective because a cybercriminal can install a Malicious Code on a computer and conduct criminal activities without any interruption.
5. Pornographic websites and other similar websites with indecent contents are not blocked.
6. Cybercafe owners have very less awareness about IT Security and IT Governance.
7. Government/ISPs/State Police (cyber cell wing) do not seem to provide IT Governance guidelines to cybercafe owners.

Cybercafé and Cybercrimes

8. Cybercafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cybercafes – one of the cybercafe owners whom we interviewed expressed a view that the police will not visit a cybercafe unless criminal activity is registered by filing an First Information Report (FIR).

- Cybercafe owners feel that police either have a very little knowledge about the technical aspects involved in cybercrimes and/or about conceptual understanding of IT security. There are thousands of cybercafes across India.
- In the event that a central agency takes up the responsibility for monitoring cybercafes, an individual should take care while visiting and/or operating from cybercafe.

Cybercafé and Cybercrimes

- Here are a few tips for safety and security while using the computer in a cybercafe:

1. Always logout
2. Stay with the computer
3. Clear history and temporary files
4. Be alert
5. Avoid online financial transactions
6. Change passwords
7. Use Virtual keyboard
8. Security warnings

Botnets: The Fuel for Cybercrime

- The dictionary meaning of Bot is “(computing) an automated program for doing some particular task, often over a network.”
- Botnet is a term used for collection of software robots, or Bots, that run autonomously and automatically.
- The term is often associated with malicious software but can also refer to the network of computers using distributed computing software.
- In simple terms, a Bot is simply an automated computer program One can gain the control of computer by infecting them with a virus or other Malicious Code that gives the access.

Botnets: The Fuel for Cybercrime

- Computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.
- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- "Zombie networks" have become a source of income for entire groups of cybercriminals.
- The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge required to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.

Botnets: The Fuel for Cybercrime

- If someone wants to start a “business” and has no programming skills, there are plenty of “Bot for sale” offers on forums.
- ‘encryption of these programs’ code can also be ordered in the same way to protect them from detection by antivirus tools.
- Another option is to steal an existing Botnet. Figure 2.8 explains how Botnets create business.
- One can reduce the chances of becoming part of a Bot by limiting access into the system.
- Leaving your Internet connection ON and unprotected is just like leaving the front door of the house wide open.

Botnets: The Fuel for Cybercrime

- One can ensure following to secure the system:
- Use antivirus and anti-Spyware software and keep it up-to-date.
- Set the OS to download and install security patches automatically.
- Use a firewall to protect the system from hacking attacks while it is connected on the Internet.
- A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications.
- Disconnect from the Internet when you are away from your computer.
- Downloading the freeware only from websites that are known and trustworthy.
- Check regularly the folders in the mail box – “sent items” or “outgoing” – for those messages you did not send.
- Take an immediate action if your system is infected.

Box 2.9 | Technical Terms
Malware: It is malicious software, designed to damage a computer system without the owner's informed consent. Viruses and worms are the examples of malware.
Adware: It is advertising-supported software, which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Few Spywares are classified as Adware.
Spam: It means unsolicited or undesired E-Mail messages
Spamdexing: It is also known as search Spam or search engine Spam. It involves a number of methods, such as repeating unrelated phrases, to manipulate the relevancy or prominence of resources indexed by a search engine in a manner inconsistent with the purpose of the indexing system.
DDoS: Distributed denial-of-service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods

Attack Vector

- An “attack vector” is a path, which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- Attack vectors enable attackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception.
- All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defences
- To some extent, firewalls and antivirus software can block attack vectors.
- However, no protection method is totally attack-proof.
- A defence method that is effective today may not remain so for long because attackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers. Refer to Box 2.10.

Attack Vector

- The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.
- In the technical terms, payload is the necessary data being carried within a packet or other transmission unit – in this scenario (i.e., attack vector) payload means the malicious activity that the attack performs.
- From the technical perspective, payload does not include the "overhead" data required to get the packet to its destination. Payload may depend on the following point of view: "What constitutes it?"
- To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include that part of the overhead data that this layer handles.

Attack Vector

- The attack vectors described here are how most of them are launched.
- **Attack by E-Mail:** The content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind. Any link that offers something “free” or tempting is a suspect.
- **Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. Attachments attempt to install their payload as soon as you open them.
- **Attack by deception**: Deception is aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor.
- Fraud, scams, and to some extent Spam, not to mention viruses, worms and such require the unwitting cooperation of the computer’s operator to succeed. Social engineering are other forms of deception that are often an attack vector too.

Attack Vector

- **Hackers**: Hackers/crackers are a formidable attack vector because, unlike ordinary Malicious Code, people are flexible and they can improvise.
- Hackers/crackers use a variety of hacking tools, heuristics, and social engineering to gain access to computers and online accounts.
- They often install a Trojan Horse to commandeer the computer for their own use.
- **Heedless guests (attack by webpage):** Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate.
- One may think he/she is doing business with someone you trust. However, he/she is really giving their personal information, like address, credit card number, and expiration date.
- They are often used in conjunction with Spam, which gets you there in the first place. Pop-up webpages may install Spyware, Adware or Trojans.

Attack Vector

- **Attack of the worms:** Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly.
- Any remote access service, like file sharing, is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses.
- **Malicious macros**: Microsoft Word and Microsoft Excel are some of the examples that allow macros.
- A macro does something like automating a spreadsheet, for example.
- Macros can also be used for malicious purposes.
- All Internet services like instant messaging, Internet Relay Chart (IRC), and P2P file-sharing networks rely on cozy connections between the computer and the other computers on the Internet.
- If one is using P2P software then his/her system is more vulnerable to hostile exploits.

Attack Vector

- **Foistware (sneakware):** Foistware is the software that adds hidden components to the system with cunning nature.
- Spyware is the most common form of foistware.
- Foistware is partial- legal software bundled with some attractive software.
- Sneak software often hijacks your browser and diverts you to some “revenue opportunity” that the foistware has set up.
- **Viruses:** These are malicious computer codes that hitch a ride and make the payload.
- Nowadays, virus vectors include E-Mail attachments, downloaded files, worms, etc.

Box 2.10 | Zero-Day Attack

A zero-day (or zero-hour) attack[17] is a computer threat which attempts to exploit computer application vulnerabilities that are unknown to anybody in the world (i.e., undisclosed to the software vendor and software users) and/or for which no patch (i.e., security fix) is available. Zero-day exploits are used or shared by attackers before the software vendor knows about the vulnerability.

Sometimes software vendors discover the vulnerability but developing a patch can take time. Alternatively, software vendors can also hold releasing the patch reason to avoid the flooding the customers with numerous individual updates. A "zero-day" attack is launched just on or before the first or "zeroth" day of vendor awareness, reason being the vendor should not get any opportunity to communicate/distribute a security fix to users of such software. If the vulnerability is not particularly dangerous, software vendors prefer to hold until multiple updates (i.e., security fixes commonly known as patches) are collected and then release them together as a package. Malware writers are able to exploit zero-day vulnerabilities through several different attack vectors.

Zero-day emergency response team (ZERT): This is a group of software engineers who work to release non-vendor patches for zero-day exploits. Nevada is attempting to provide support with the Zeroday Project at www.zerodayproject.com, which purports to provide information on upcoming attacks and provide support to vulnerable systems. Also visit the weblink http://www.isotf.org/zert to get more information about it.

Cloud Computing

- The growing popularity of cloud computing and virtualization among organizations have made it possible, the next target of cybercriminals.
- Cloud computing services, while offering considerable benefits and cost savings, move servers outside the organizations security perimeter, which make it easier for cybercriminals to attack these systems.
- Cloud computing is Internet ("cloud")-based development and use of computer technology ("computing").
- The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer networks.
- Cloud computing is a term used for hosted services delivered over the Internet.

Cloud Computing

- A cloud service has three distinct characteristics which differentiate it from traditional hosting:

1. It is sold on demand – typically by the minute or the hour;
2. It is elastic in terms of usage – a user can have as much or as little of a service as he/she wants at any given time;
3. The service is fully managed by the provider – a user just needs PC and Internet connection. Significant innovations into distributed computing and virtualization as well as improved access speed over the Internet have generated a great demand for cloud computing.

Why Cloud Computing?

- The cloud computing has following advantages.
- Applications and data can be accessed from anywhere at any time. Data may not be held on a hard drive on one user's computer.
- It could bring hardware costs down. One would need the Internet connection.
- Organizations do not have to buy a set of software or software licenses for every employee and the organizations could pay a metered fee to a cloud computing company.
- Organizations do not have to rent a physical space to store servers and databases. Servers and digital storage devices take up space.
- Cloud computing gives the option of storing data on someone else's hardware, thereby removing the need for physical space on the front end.
- Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware. The cloud computing services can be either private or public.

Why Cloud Computing?

- **Types of Services**
- Services provided by cloud computing are as follows:
- **Infrastructure-as-a-service (IaaS):** It is like Amazon Web Services that provide virtual servers with unique IP addresses and blocks of storage on demand.
- Customers benefit from an Application Programmable Interface (API) from which they can control their servers.
- As customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.
- **Platform-as-a-service (PaaS):** It is a set of software and development tools hosted on the provider's servers. Developers can create applications using the provider's APIs.
- Google Apps is one of the most famous PaaS providers. Developers should take notice that there are not any interoperability standards; therefore, some providers may not allow you to take your application and put it on another platform.

Why Cloud Computing?

- **Software-as-a-service (SaaS):** It is the broadest market. In this case, the provider allows the customer only to use its applications. The software interacts with the user through a user interface. These applications can be anything from Web-based E-Mail to applications such as Twitter or Last.fm.

- **Cybercrime and Cloud Computing**
- Nowadays, prime area of the risk in cloud computing is protection of user data. Although cloud computing is an emerging field, the idea has been evolved over few years.
- Risks associated with cloud computing environment are as follows:

1. Elevated user access	Any data processed outside the organization brings with it an inherent level of risk
2. Regulatory compliance	Cloud computing service providers are not able and/or not willing to undergo external assessments.
3. Location of the data	User doesn't know where the data is stored or in which country it is hosted.
4. Segregation of data	Data of one organization is scattered in different locations
5. Recovery of the data	In case of any disaster, availability of the services and data is critical.
6. Information security violation reports	Due to complex IT environment and several customers logging in and logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity
7. Long-term viability	In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at the stake.