Introduction to Cybercrime

- “Cyber security is the protection of internet-connected systems, including hardware, software and data, fr cyber attacks”.
- “Cybersecurity” means protecting information, equipment, devices, computer, computer resource, from unauthorized access, use, disclosure, disrupti modification or destruction.
- Almost everyone is aware of the rapid growth of the

Introduction to Cybercrime

- These activities involve the use of computers, the Internet, cyberspace and the worldwide web (WWW).
- Interestingly, cybercrime is not a new phenomena; the first recorded cybercrime took place in the year 1820.
- It is one of the most talked about topics in the recent years.
- Based on a 2008 survey in Australia, the below shows the cybercrime trend.
- Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.
- Given the unrestricted number of free websites, the Internet has undeniably opened a new way of exploitation known as cybercrime.

Introduction to Cybercrime

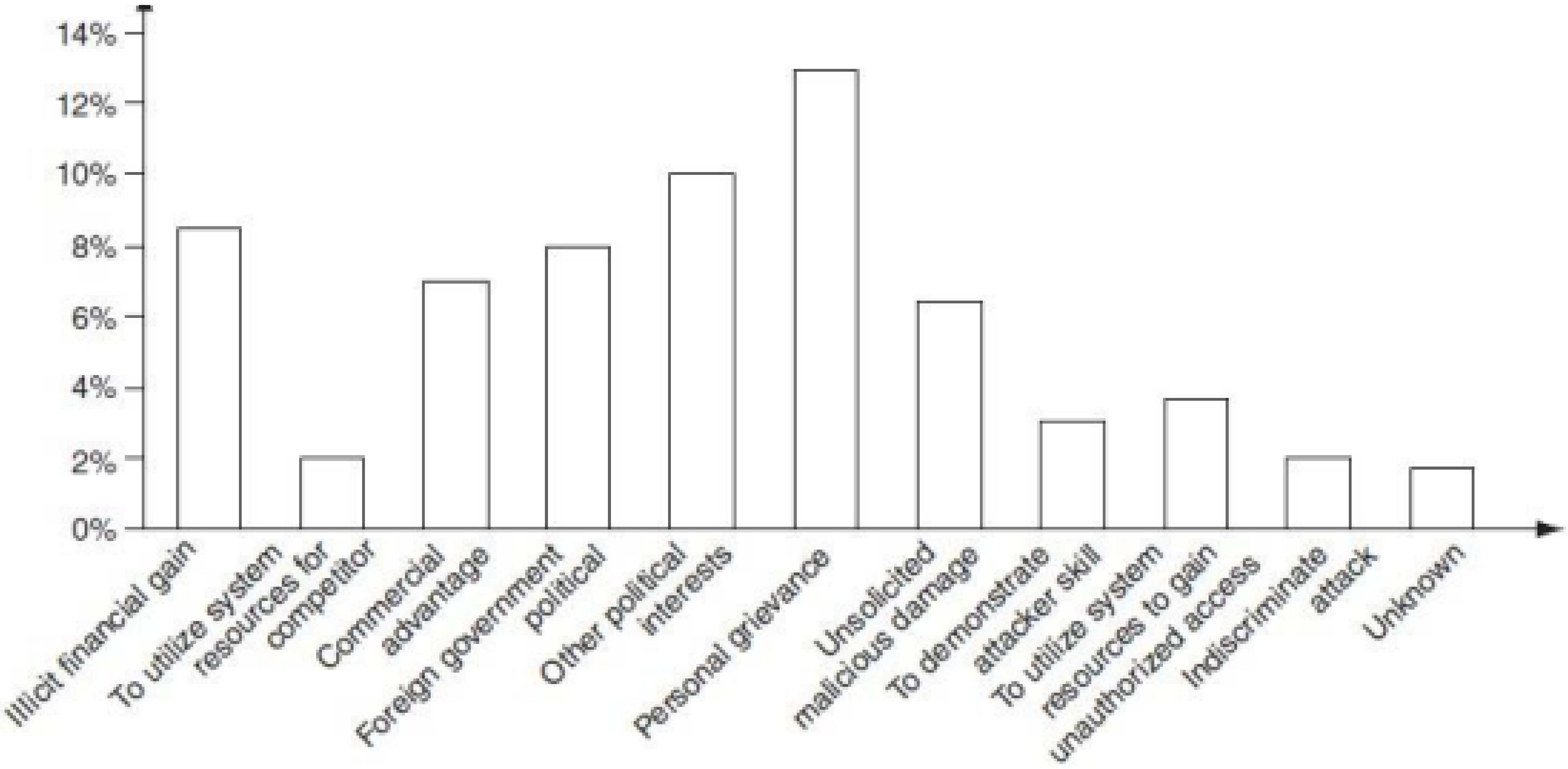


Figure: Cybercrime Trend

CYBERCRIME: DEFINITION AND ORIGINS OF THE WORD

- “A crime conducted in which a computer was directly and significantly instrumental is called as a Cybercrime.”
- Any illegal act where a special knowledge of computer technology is essential for its perpetration (to commit a crime), 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, damage and demands for money.

CYBERCRIME: DEFINITION AND ORIGINS OF THE WORD

- “Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them”.
- The term “cybercrime” relates to a number of other terms that may sometimes be used to describe crimes committed using computers.
- Computer-related crime
- Computer crime
- Internet crime
- E-crime
- High-tech crime, etc. are the other synonymous terms.

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.”
- **Cybernetics:** Cybernetics deals with information and its use. 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
- **Phishing:** Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords, credit card information from users etc.

Important Definitions related to Cyber Security

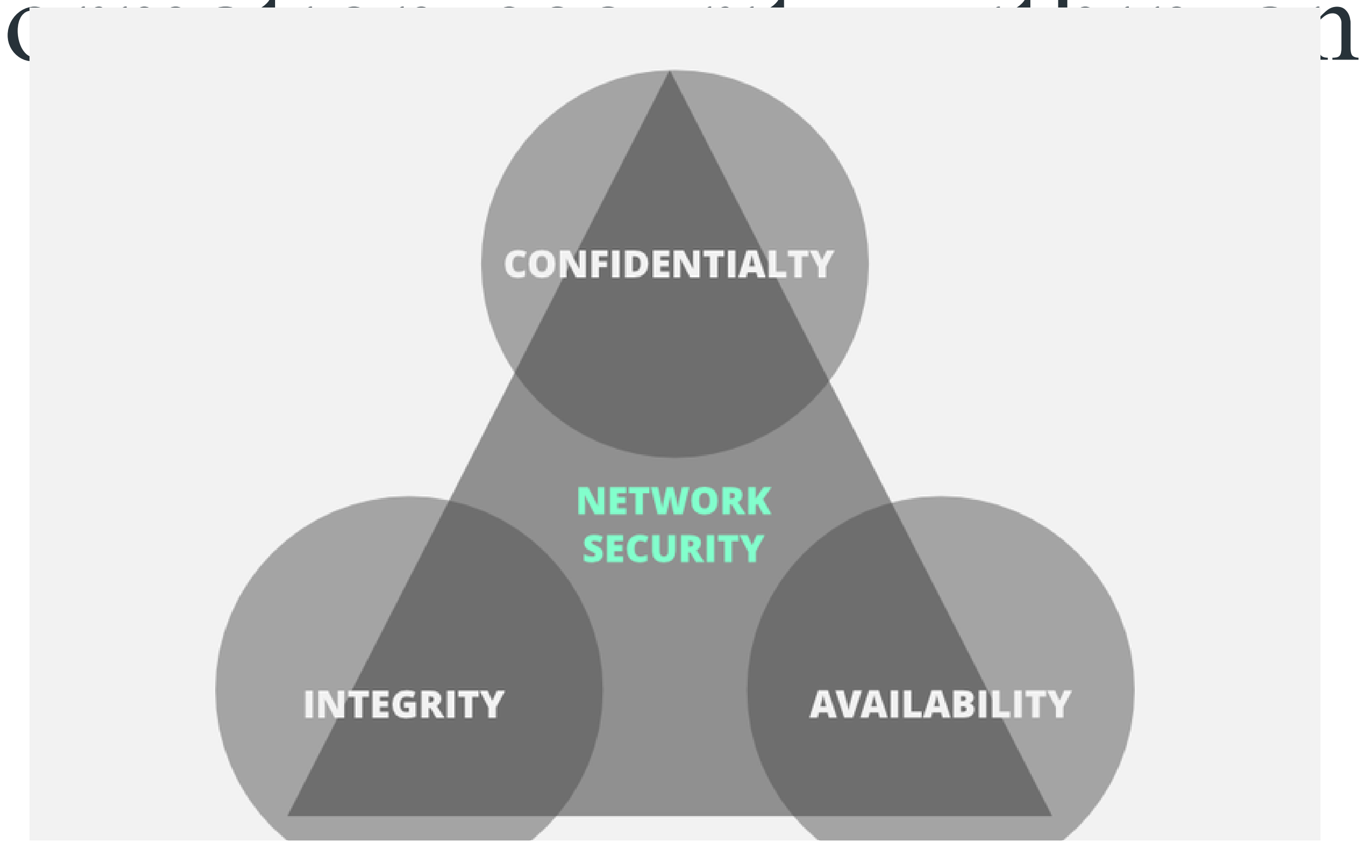
- **Cyberspace:** “cyberspace” is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data. Cyberspace is most definitely a place where you chat, explore, research and play.
- **Cybersquatting:**Cybersquatting 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.
- **Cyberwarfare:**These type of Cyber attacks are often presented as threat to military forces and the Internet has major implications for espionage and warfare.

INFORMATION SECURITY

- INFORMATION SECURITY: Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual prop When talking about network security, the **CIA** triad is one of the most important models which is designed to guide policies for information security within an organization.

  CIA stands for :

1. Confidentiality
2. Integrity
3. Availability



INFORMATION SECURITY

1. **Confidentiality:**The term 'confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. The property that data or information is not made available or disclosed to unauthorized persons or processes.

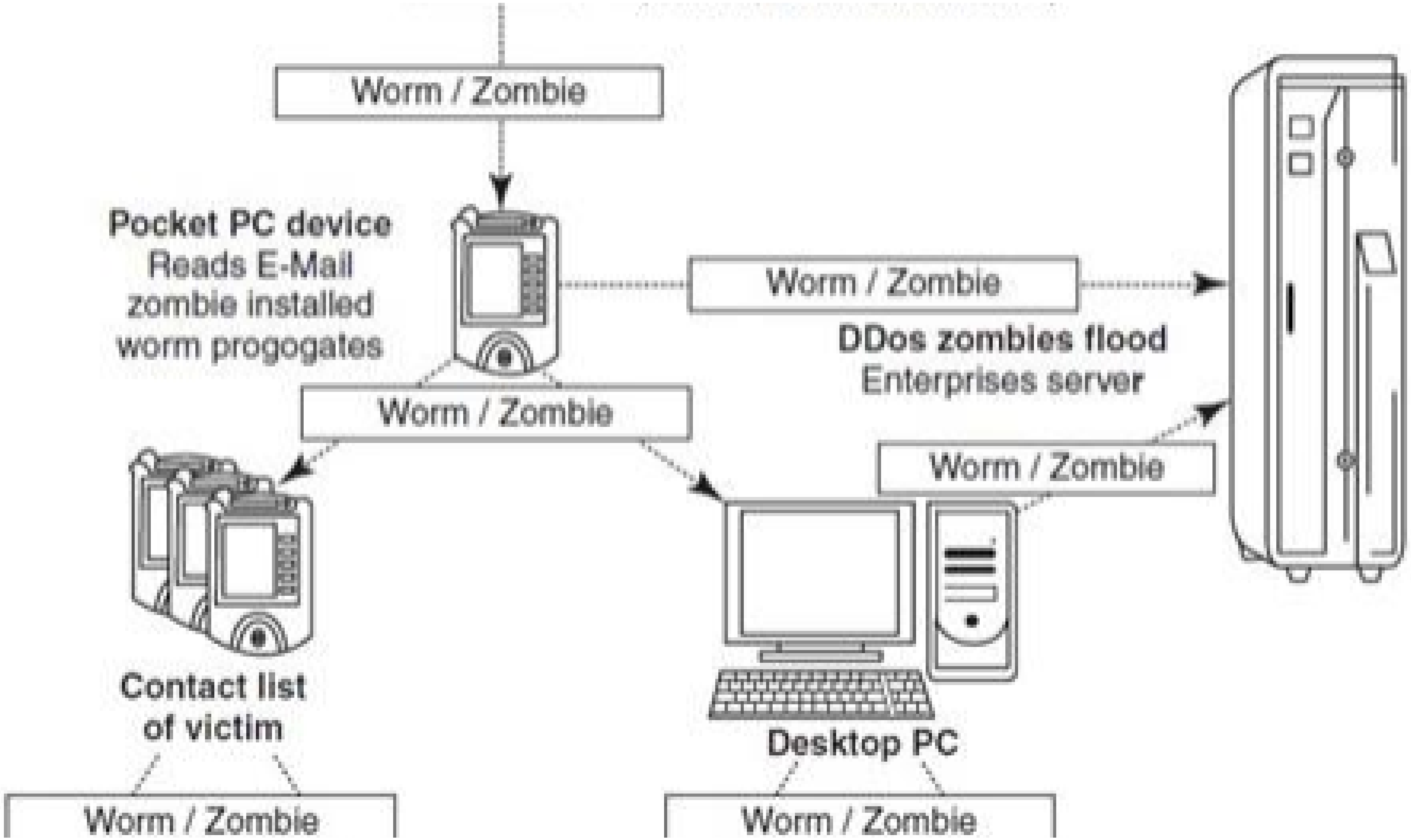
INFORMATION SECURITY

The Botnet Menace: A group of computers that are controlled by software containing harmful programs, without their users' knowledge is called as Botnet. 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. Below figure shows how a “zombie” works.

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.

INFORMATION SECURITY



WHO ARE CYBERCRIMINALS

Cybercrime involves such activities

- credit card fraud
- cyberstalking
- defaming another online
- gaining unauthorized access to computer systems
- ignoring copyright, software licensing and trademark protection;
- overriding encryption to make illegal copies;
- software piracy and stealing another's identity (known as identity theft) to perform criminal acts.

Types of Cybercriminals

Types of Cybercriminals:

1. Type I: Cybercriminals – hungry for recognition
   - Hobby hackers;
   - IT professionals (social engineering is one of the biggest threat);
   - Politically motivated hackers;
   - Terrorist organizations.
2. Type II: Cybercriminals – not interested in recognition

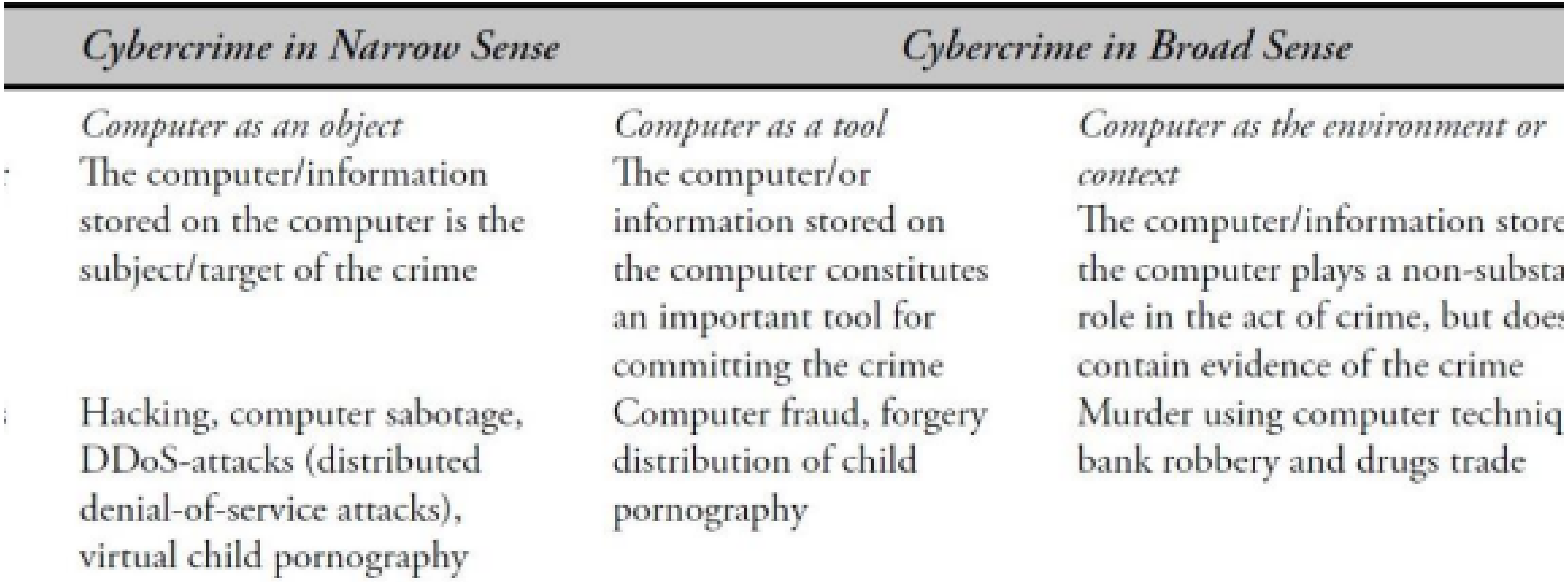
- Psychological perverts;

Types of Cybercriminals

3. Type III: Cybercriminals – the insiders

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

CLASSIFICATIONS OF CYBERCRIMES



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

Table: Classifying Cybercrimes

A GLOBAL PERSPECTIVE ON CYBERCRIMES

The linkage of cybersecurity and critical infrastructure protection has become a big issue as a number of countries have began assessment of threats, vulnerabilities and started exploring mechanisms to redress them. Recently, there have been a number of significant developments such as 1. August 4, 2006 Announcement: The US Senate ratifies CoE Convention on Cyber Crime. The convention targets hackers, those spreading destructive computer viruses, those using the Internet for the sexual exploitation of children or the distribution of racist material, and terrorists attempting to attack infrastructure facilities or financial institutions.

A GLOBAL PERSPECTIVE ON CYBERCRIMES

Cybercrime is a growing global issue that affects individuals, businesses, and governments around the world. Cybercrime is a term used to describe criminal activities that are committed using computers or the internet. This can include activities such as hacking, phishing, malware distribution, online fraud, and identity theft, among others. In this answer, we will provide a global perspective on cybercrime, including its impact, prevalence, and prevention.

A GLOBAL PERSPECTIVE ON CYBERCRIMES

Impact of Cybercrime:

The impact of cybercrime can be significant, both in terms of financial losses and damage to reputation. According to a report by the Center for Strategic and International Studies, the global cost of cybercrime was estimated to be around $600 billion in 2017. This includes costs associated with stolen assets, lost productivity, and recovery from attacks. In addition to financial losses, cybercrime can also result in damage to reputation, loss of intellectual property, and disruption of critical infrastructure.

A GLOBAL PERSPECTIVE ON CYBERCRIMES

Prevalence of Cybercrime:

Cybercrime is a widespread issue that affects individuals, businesses, and governments around the world. The number of cyber attacks has been steadily increasing over the years, with some estimates suggesting that there are around 300,000 new malware samples being detected every day. According to the 2020 Cost of Cybercrime Study by Accenture, the average number of security breaches experienced by organizations increased by 11% between 2018 and 2019. Cybercrime is also becoming more sophisticated, with the emergence of new threats such as ransomware and advanced persistent threats (APTs).

A GLOBAL PERSPECTIVE ON CYBERCRIMES

Prevention of Cybercrime:

Preventing cybercrime requires a multi-faceted approach that includes both technical and non-technical measures. Technical measures may include implementing strong passwords, using encryption, regularly updating software and hardware, and using anti-malware software. Non-technical measures may include raising awareness about cyber threats and providing training to individuals and organizations on how to prevent and respond to cyber attacks.

A GLOBAL PERSPECTIVE ON CYBERCRIMES

Governments can also play a role in preventing cybercrime by enacting laws and regulations that deter cyber criminals and hold them accountable for their actions.
In conclusion, cybercrime is a growing global issue that requires a
concerted effort from individuals, businesses, and governments to
prevent and mitigate its impact. By raising awareness about the risks of cybercrime and implementing effective prevention measures, we can help to ensure that the internet remains a safe and secure place for everyone.

CYBERCRIME ERA: SURVIVAL MANTRA FOR THE NETIZENS

Therefore, by corollary, “Netizen” is someone who spends considerable time online and also has a considerable presence online (through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms). The 5P Netizen mantra for online security is:

a. Precaution b. Prevention c. Protection d. Preservation e. Perseverance

For ensuring cyber safety, the motto for the “Netizen” should be “Stranger is Danger!” If you protect your customer’s data, your employee’s privacy and your own company, then you are doing your job in the grander scheme of things to regulate and enforce rules on the Net through our community.

CYBERCRIME ERA: SURVIVAL MANTRA FOR THE NETIZENS

- NASSCOM urges that cybercrime awareness is important, and any matter should be reported at once.
- This is the reason they have established cyberlabs across major cities in India.

Cyber Offenses

How Criminals Plan the 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

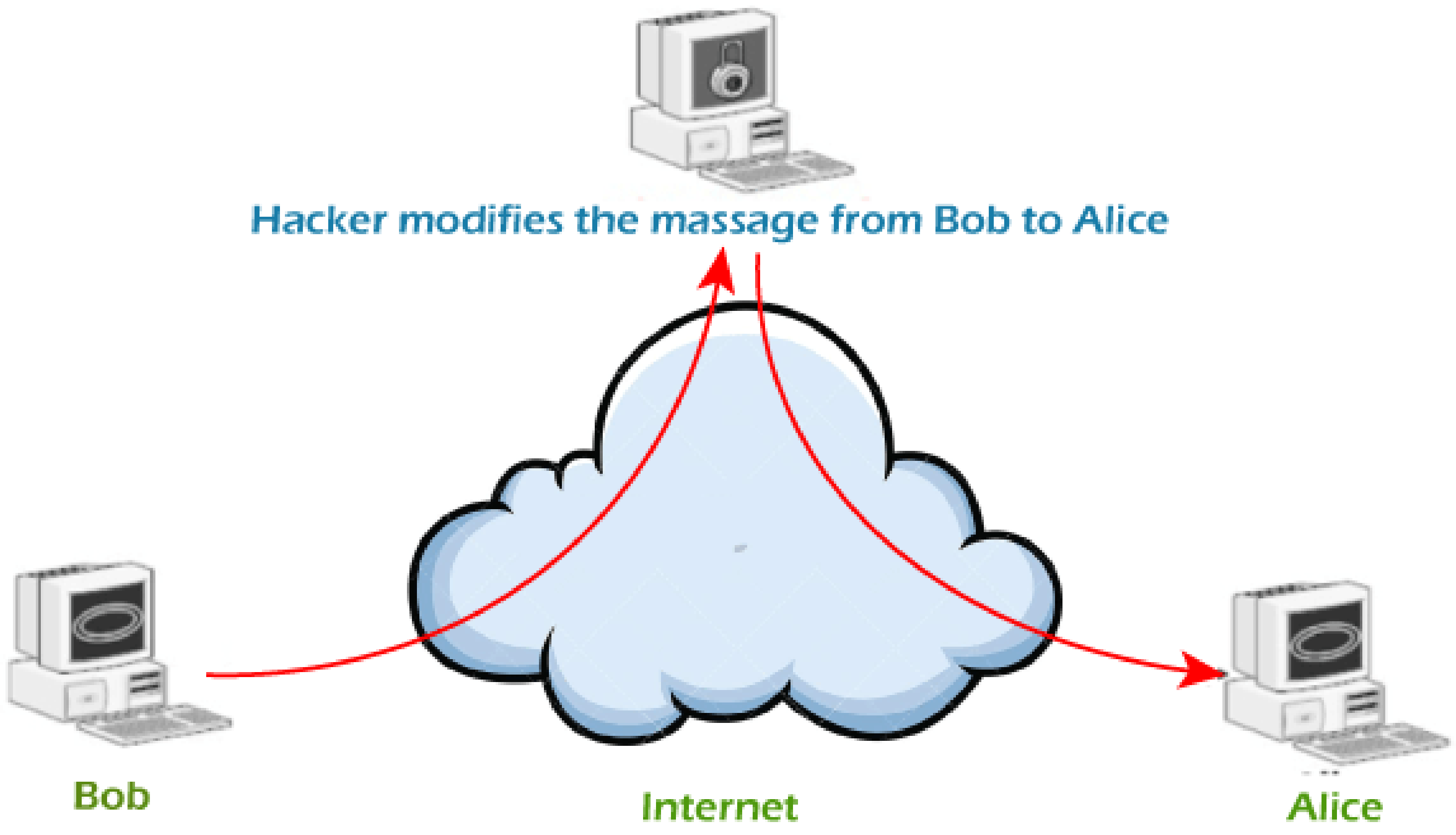
 Active attacks are usually used to alter the system (i.e., computer network) whereas passive attacks attempt to gain information about the target.

 Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to violation of confidentiality.

How Criminals Plan the Attacks

1.Active attacks

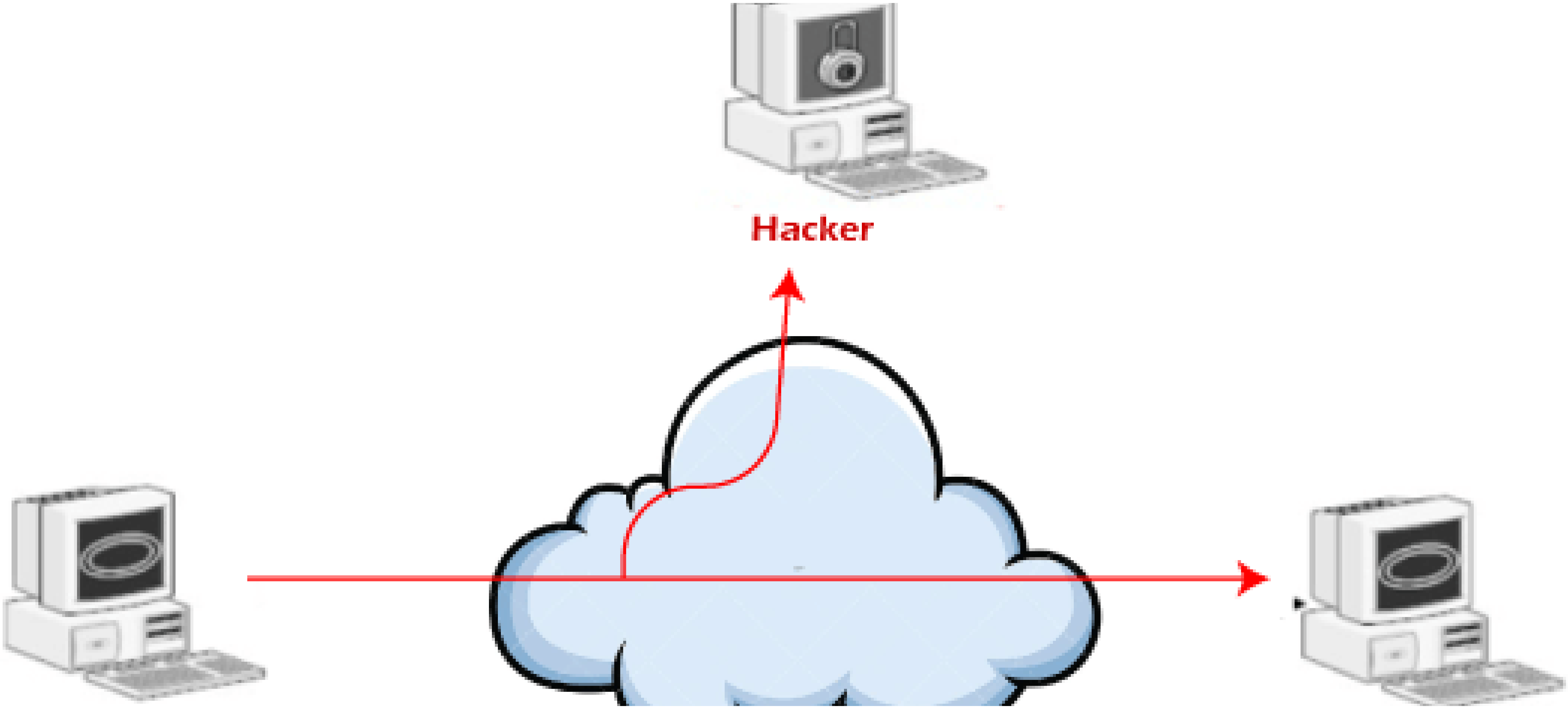
In active attacks, the attacker intercepts the connection and efforts to modify the message's content. It is dangerous for integrity and availability of the message. Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service. The system resources can be changed due to active attacks. So, the damage done with active attacks can be harmful to the system and its resources.



How Criminals Plan the Attacks

2.Passive attacks

In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes. The attacker does not try to change the information or content he/she gathered. Although passive attacks do not harm the system, they can be a danger for the confidentiality of the message.In the below image, we can see the process of passive attacks.



How Criminals Plan the Attacks

3.**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:

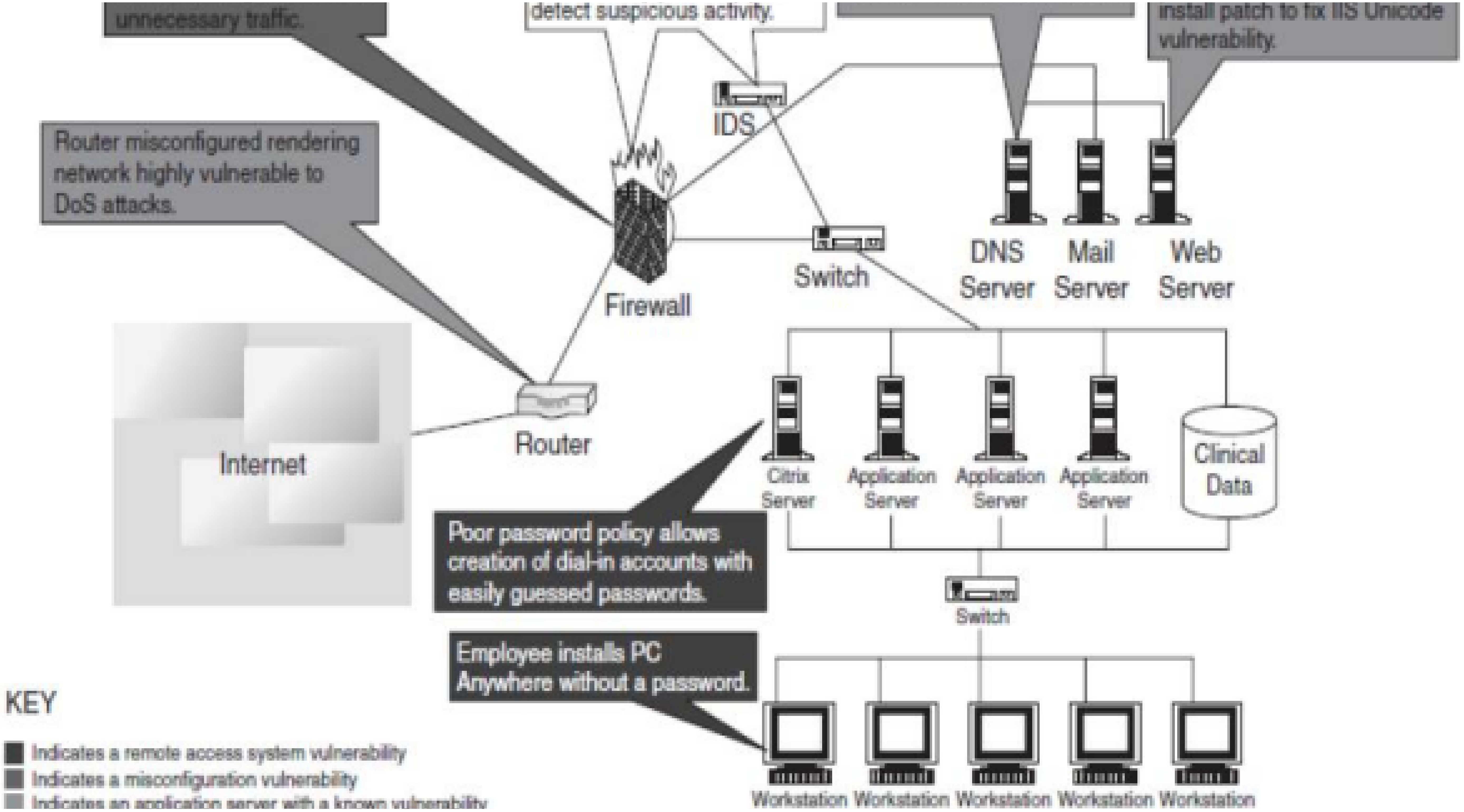
1. Port scanning: Identify open/close ports and services.
2. Network scanning: Understand IP Addresses and related information about the computer network systems.
3. Vulnerability scanning: Understand the existing weaknesses in the system.

How Criminals Plan the Attacks

4. Attack (Gaining and Maintaining the System Access) After the scanning and enumeration, the attack is launched using the following steps:

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

How Criminals Plan the Attacks



unnecessary traffic.

detect suspicious activity.

install patch to fix IIS Unicode vulnerability.

Router misconfigured rendering network highly vulnerable to DoS attacks.

Poor password policy allows creation of dial-in accounts with easily guessed passwords.

Employee installs PC Anywhere without a password.

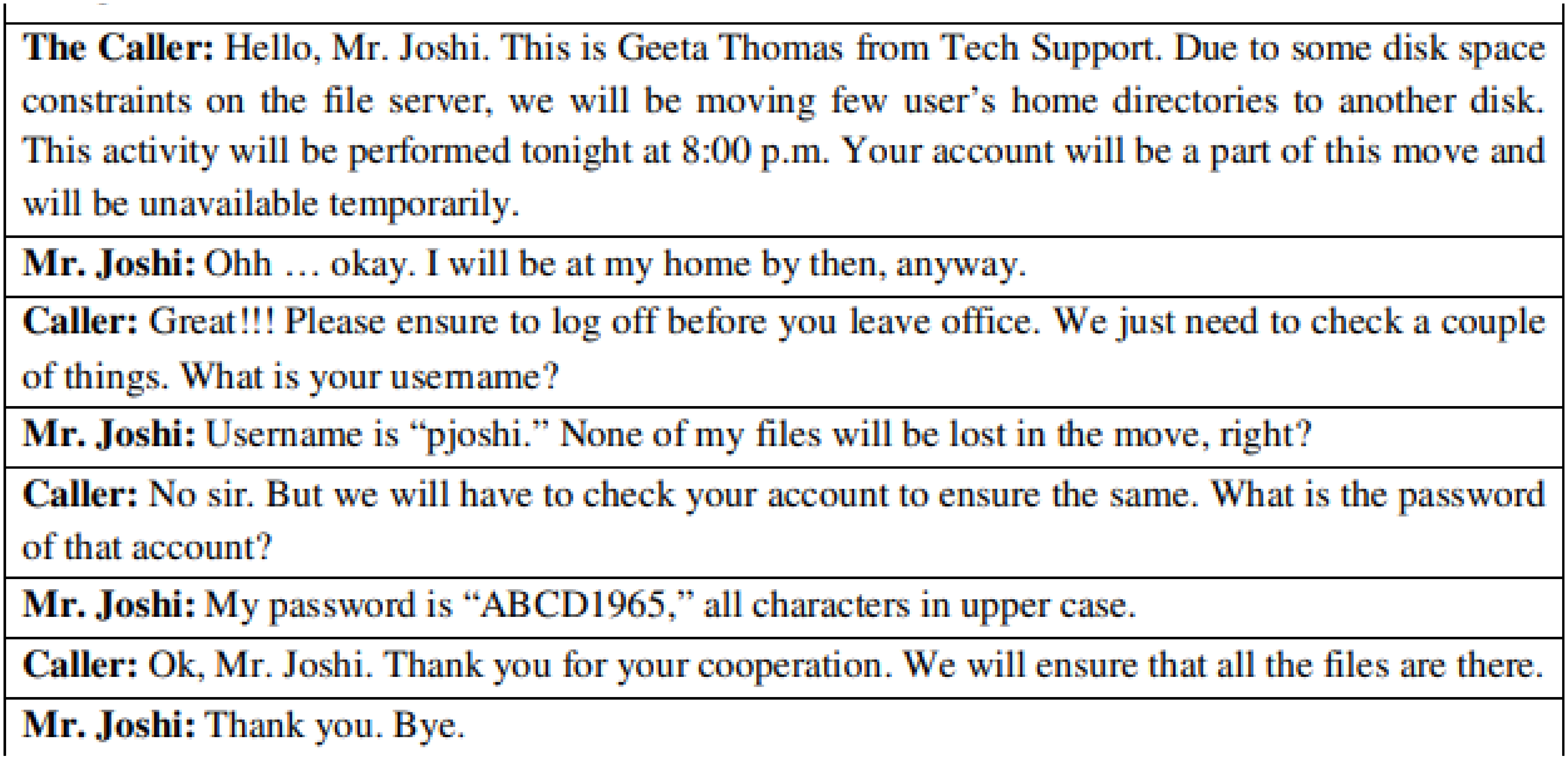
KEY

■ Indicates a remote access system vulnerability
▩ Indicates a misconfiguration vulnerability
▨ Indicates an application server with a known vulnerability

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.
- It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.

Social engineering



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 usemame?

Mr. Joshi: Usemame 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 files are there.

Mr. Joshi: Thank you. Bye.

Social engineering

Classification of Social Engineering

- Human-Based Social Engineering
- Posing as an important user
- Using a third person:
- Calling technical support
- Shoulder surfing

Computer-Based Social Engineering

- Fake E-Mails
- E-Mail attachments
- Pop-up windows

Cyberstalking

- 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 behavior 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 refers to the use of Internet and/or other electronic communications devices to stalk another person.

Types of Stalkers.There are primarily two types of stalker

1. Online stalkers
2. Offline stalkers

Cyberstalking

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.

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.

Cybercafe 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 practiced 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.

Cybercafe and Cybercrimes

- Cybercriminals prefer cybercafes to carry out their activities.

- The criminals tend to identify one particular personal computer (PC) to prepare it for their use.

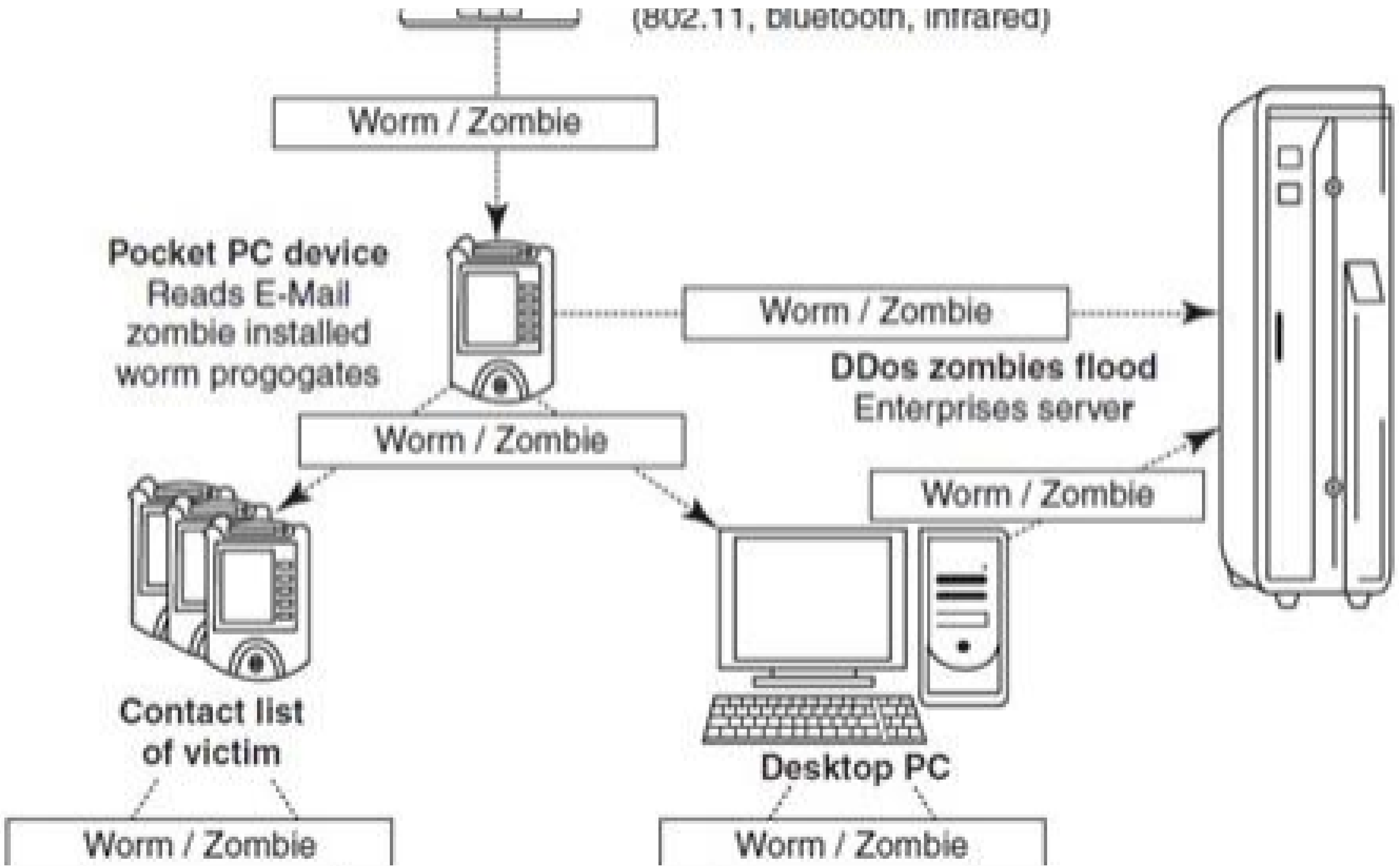
- Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target.

- Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week.

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



Botnets: The Fuel for Cybercrime

- 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.

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 defenses.
- To some extent, firewalls and antivirus software can block attack vectors.
- However, no protection method is totally attack-proof.

Attack Vector

- The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware.
- The attack vectors described here are how most of them are launched.
- Attack by E-Mail:Reside in spam
- 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.
- Hackers:Hackers/crackers use variety of hacking tools, heuristics.

Attack Vector

- 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.
- Foistware (sneakware): Foistware is the software that adds hidden components to the system with cunning nature. Spyware is the most common form of foistware.
- Attack of the worms: Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly