Cyber Security

Module 1 & Module 2

by Dr. DEEP SUMAN DEV

How many of you have done this?

- Your password is the word “password” or the digits “123”or your first name, etc.
- You leave your computer, phone, or tablet unattended at a coffee shop, or open and available when other people are in your home.
- You click links in an e-mail indiscriminately, without stopping to think (or find out) if they are legitimate.
- You store data indiscriminately in “the cloud” without considering the ramifications of doing so and/or the policies of your workplace.
- You don’t change your password even after you think someone else might have learned it.
- You ignore warnings from corporate or consumer IT professionals concerning password strength, reuse, and retirement.
- You don’t have a pass-code on your smartphone, even though you keep a list of account numbers or passwords on it.
- You connect to open, public Wi-Fi networks and transmit sensitive data over these unsecured channels.
- You visit “bad neighborhoods” on the Web, entering your e-mail address, password, and other private information in an effort to get free software, music, or movies.
- You use an ancient computer without updating your operating system or software applications.

Why Cyber Security??

- Cyber security is the practice of protecting systems, networks, and programs from digital attacks.

- These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information;

- extorting money from users; or interrupting normal business processes.

Why is Cyber Security important?

- In today’s connected world, everyone benefits from advanced cyber defense programs. At an individual level, a cyber security attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos.

- Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

- Everyone also benefits from the work of cyber threat researchers, like the team of 250 threat researchers at Talos, who investigate new and emerging threats and cyber attack strategies.

- They reveal new vulnerabilities, educate the public on the importance of cyber security, and strengthen open source tools. Their work makes the Internet safer for everyone.

WHY CYBER ATTACKS?

- Technology Dependency
- Increased Automation
- Upcoming Technologies like IoT, IIoT, IoE, AI
- Cyber Attacks include

- Financial Scams and Frauds
- Hacking
- Downloading copyrighted content
- Illegal pornographic content

- Viruses
- Cyber stalking
- Crimes against minorities
- Against LGBTQ

CIA Triad

- Confidentiality
- Integrity
- Availability

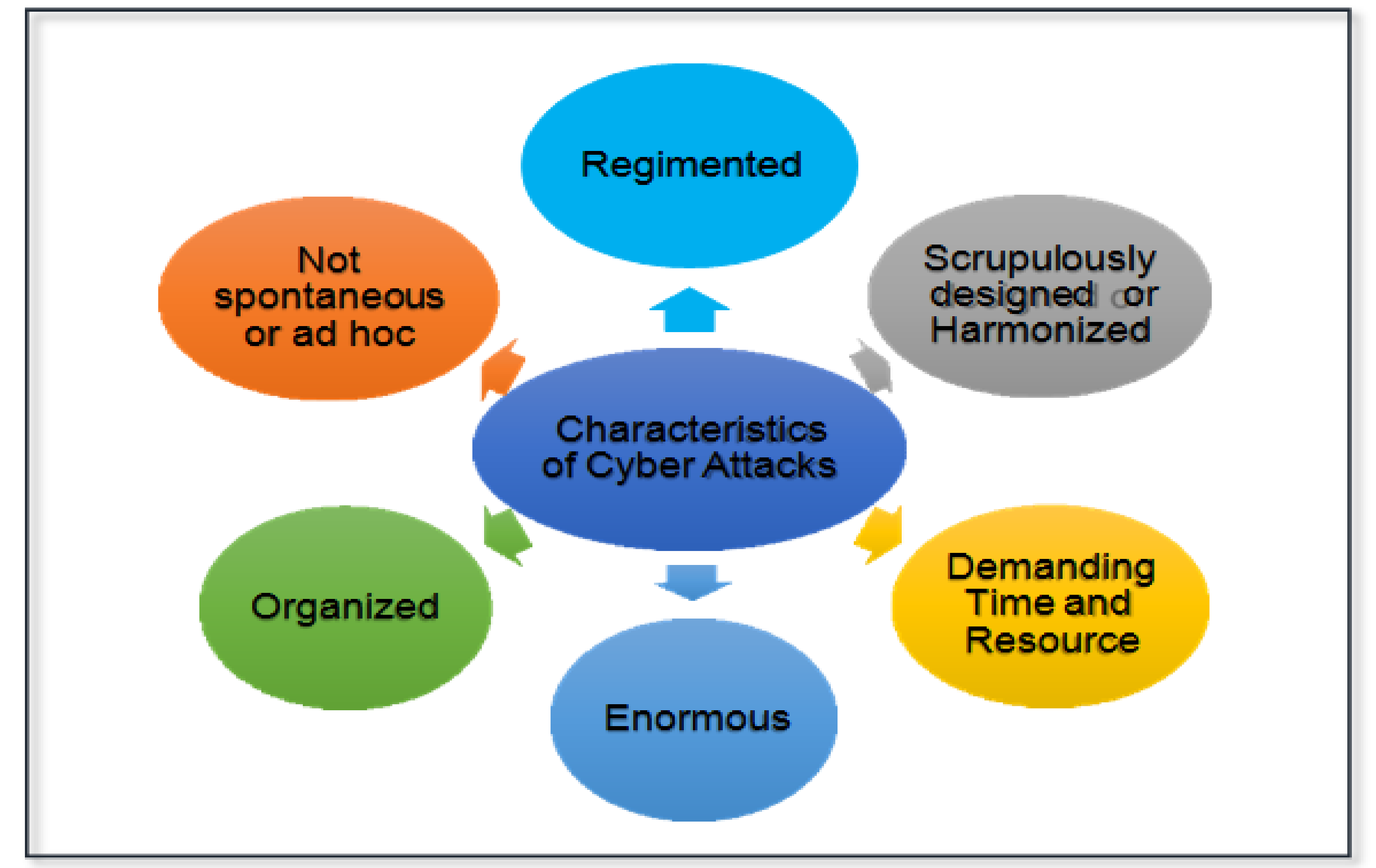
WHAT IS CYBER ATTACK?

- **Cyber Attacks** are deliberate exploitation of computer systems, resources, networks and technology connected through World Wide Web.
- It compromises data by injecting **Malicious Code** or **Logic** into the actual code or data .
- The **Compromised Data** leads to cybercrimes such as,

- Identity theft
- Fraud
- Extortion
- Malware
- Pharming
- Phishing

- Spamming
- Spoofing
- Spying
- DoS & DDOS
- H/W theft
- Message abuse

CHARACTERISTICS OF CYBER ATTACKS


Characteristics of Cyber Attacks
Regimented
Scrupulously designed or Harmonized
Demanding Time and Resource
Enormous
Organized
Not spontaneous or ad hoc

CHARACTERISTICS OF CYBER ATTACKS

- **Regimented**

  It compromises the functionality of the organization with severe damage

- **Scrupulously Designed or Harmonized**

  To infect the system, the attackers expect the process to be sequenced or methodic-use ordered steps to achieve what they exactly need so that they get benefited in time

- **Demanding Time and Resource**

  Planning for an attack is made in advance - it needs lot of time and more money to organize

CHARACTERISTICS OF CYBER ATTACKS

- **Enormous**

  initiated at large scale to infect billions of computers worldwide causing large volume of data loss and financial loss

- **Organized**

  organized methods to infect the system very quickly and easily, to get more efficient results, they use logically organized methods

- **Not Spontaneous or Adhoc**

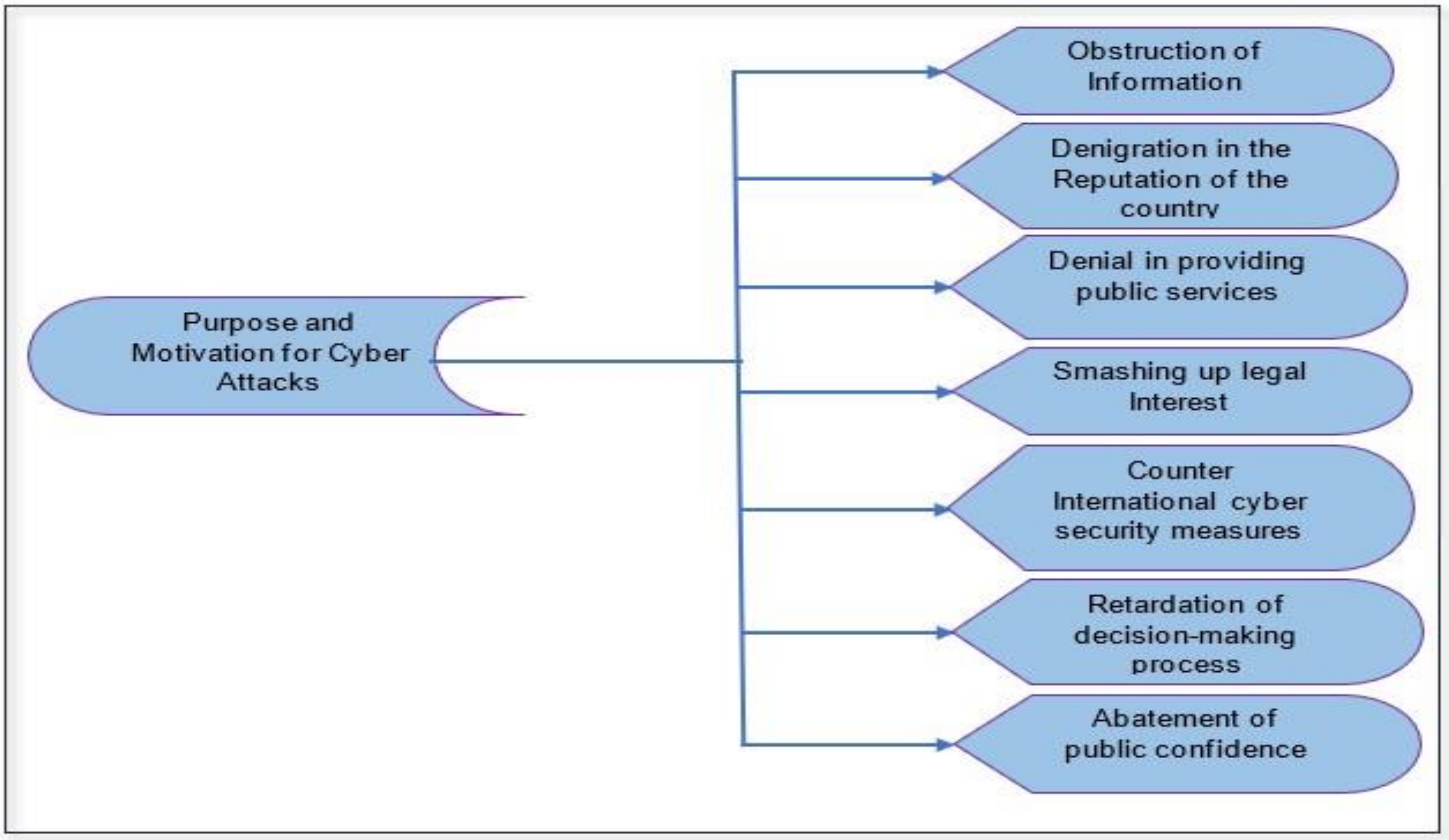
  made with purpose and care to cause maximum damage to the network or system

“Cyber Attacks are growing more stronger and more sophisticated”

PURPOSE AND MOTIVATION FOR CYBER ATTACKS

- Cyber Attacks **mainly target the information or data**
  - **Financial organization websites**
  - **News**
  - **Media websites**
  - **Military/ Defense department websites and**
  - **Government websites**

PURPOSE AND MOTIVATION FOR CYBER ATTACKS



Purpose and Motivation for Cyber Attacks

- Obstruction of Information
- Denigration in the Reputation of the country
- Denial in providing public services
- Smashing up legal Interest
- Counter International cyber security measures
- Retardation of decision-making process
- Abatement of public confidence

PURPOSE AND MOTIVATION FOR CYBER ATTACKS

- **Obstruction of Information**
- Whenever there is a need for specific data or information from any organization or from any websites the aim of the hacker is **blocking the access to that important information**
- With the authorized user's identity, the attacker blocks the access to the information and further compromise the capability of the organization for upcoming events
- **Denigration in the Reputation of the country**
- The motivation for the cyber attack is to **degrade the reputation of the organization intern and further the country**
- Every country has the competencies due to technological development which improves the productivity and values among other developing countries

PURPOSE AND MOTIVATION FOR CYBER ATTACKS

- **Denial in providing public services**
  - Attacker can cause disruption in any domains such as stock markets, banking, airline services and railway services by blocking access to valuable information for any authorized users in their organization
- **Smashing up legal Interest**
  - The well recognized organization's networks are smashed up to get the benefit of their favored organization is the known motives for cyber attack
  - To deal with such scenarios the well-defined security goals must be present in the organization

PURPOSE AND MOTIVATION FOR CYBER ATTACKS

- **Counter International cyber security measures**

- Hackers who initiate the cyber attacks are mainly concentrating to challenge or defeat the initiatives or measures taken by the international cyber security community to stop and prevent the cyber attacks
- Attackers do this by hiding their malicious code within some normal program to bypass the security scan and also, to increase the complexity of their attack patterns

- **Retardation of decision-making process**

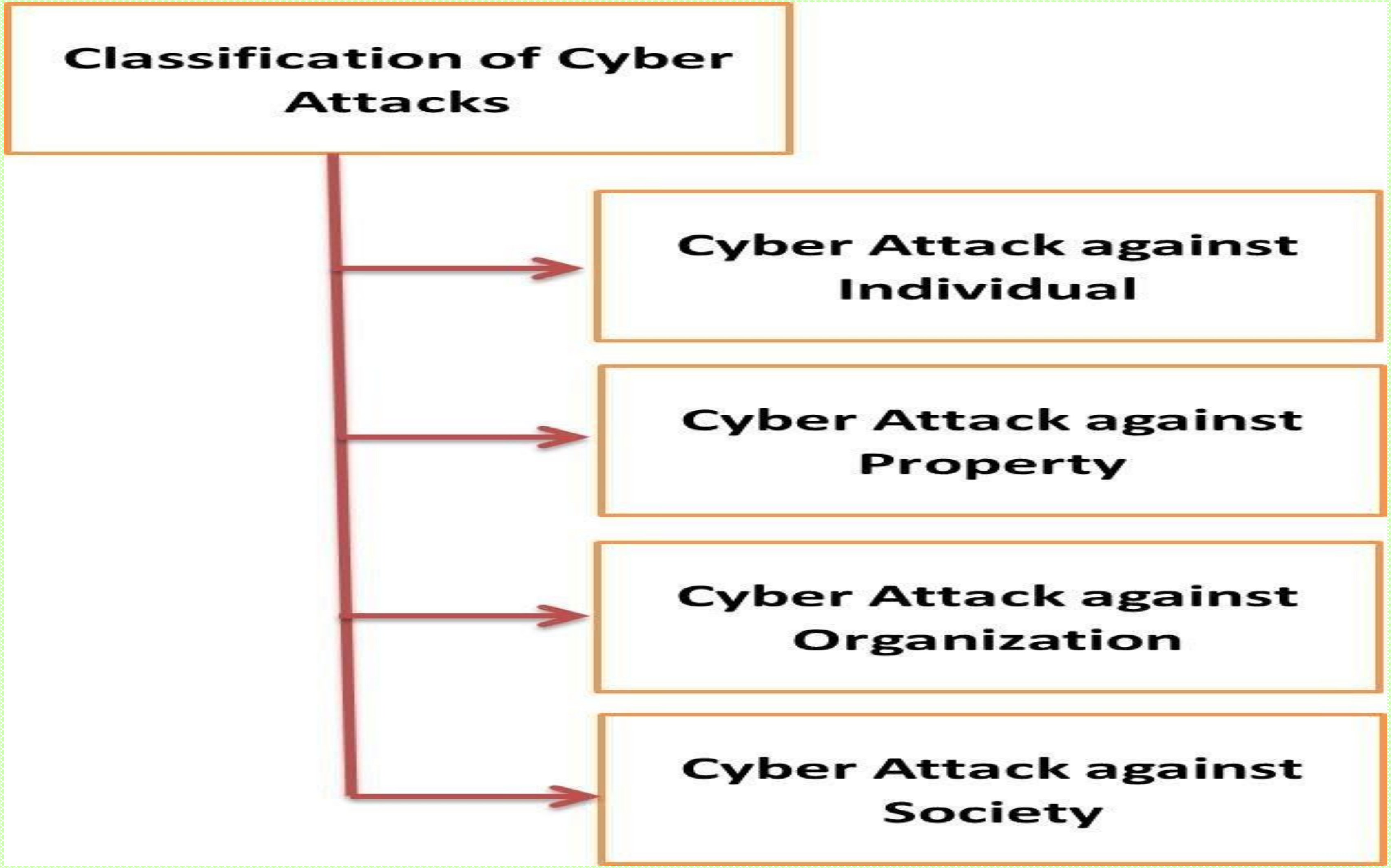
- In emergency services, military and services the cyber attacks play major role
- It causes delay in decision making processes like activation of life support system in hospital which may cause death of patients and the tactical deployment in military defeats

PURPOSE AND MOTIVATION FOR CYBER ATTACKS

➢ **Abatement of public confidence**

- Public lose their confidence about the safety, security and trustworthiness on the organization due to the stealing or hacking of their information

GENERAL CLASSIFICATION OF ATTACKS



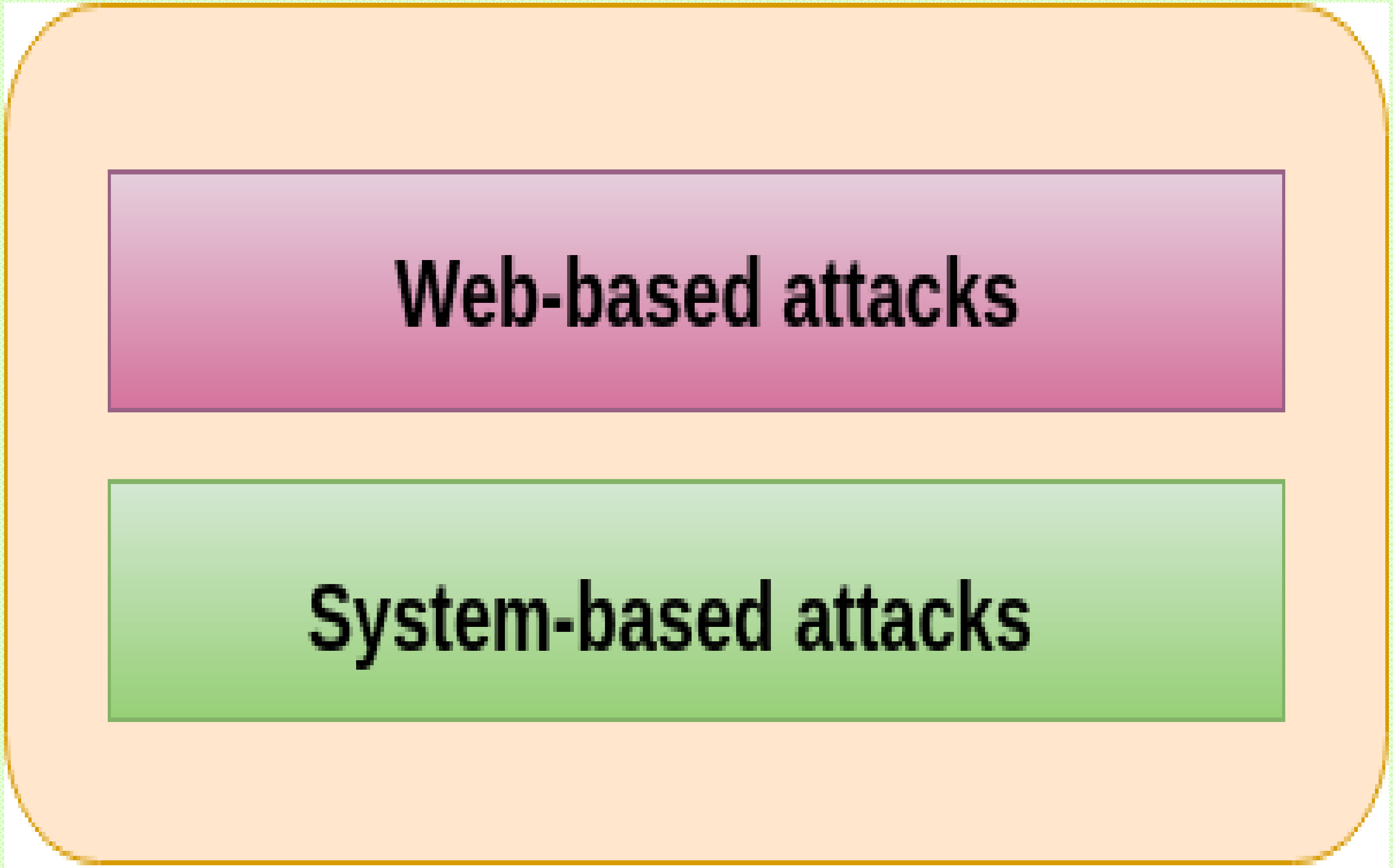
Classification of Cyber Attacks

Cyber Attack against Individual

Cyber Attack against Property

Cyber Attack against Organization

Cyber Attack against Society



Classification of Cyber attacks

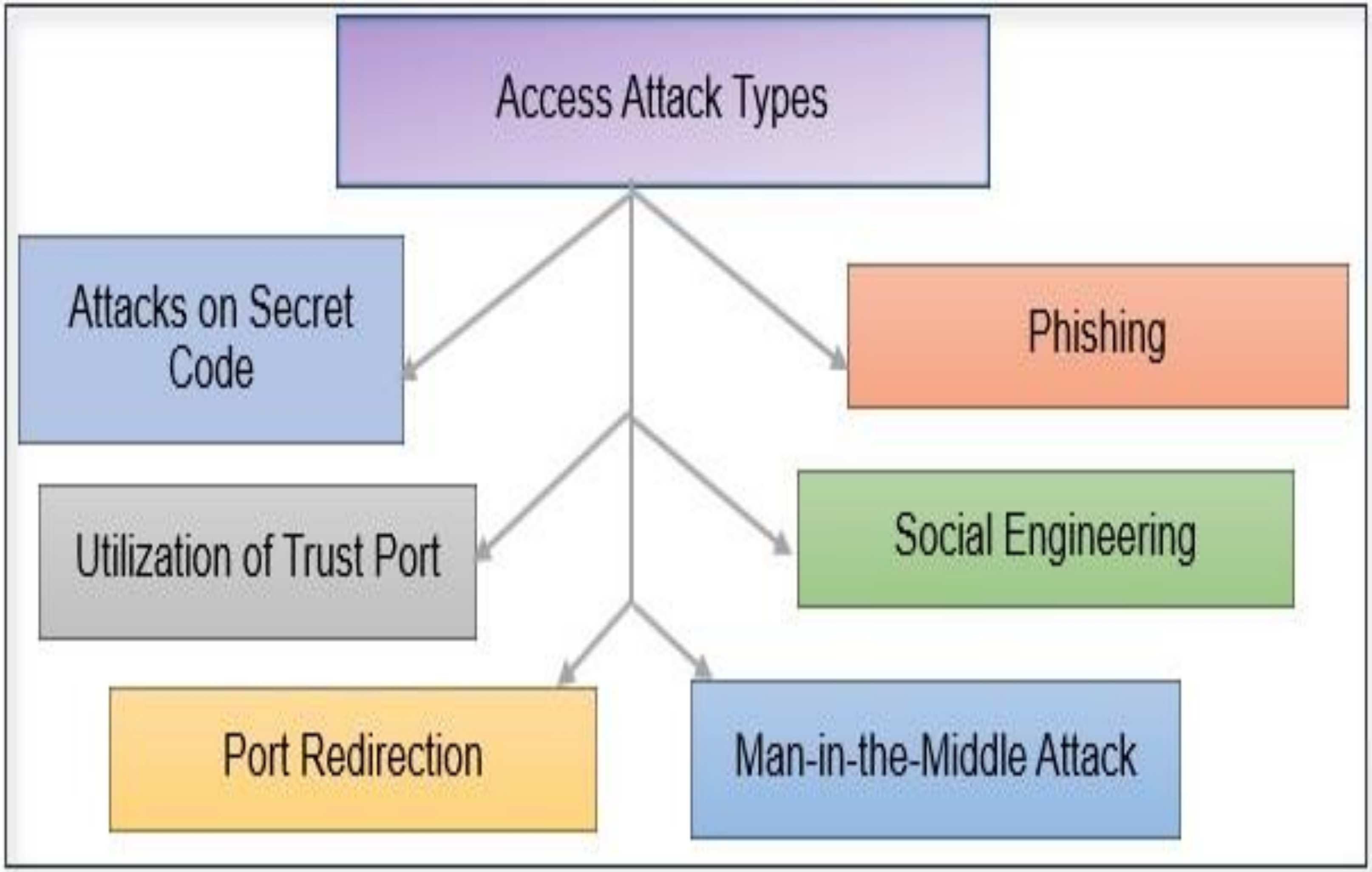
Web-based attacks

- These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-
  - **Injection attacks**
  - **DNS Spoofing**
  - **Session Hijacking**
  - **Phishing**
  - **Brute force**
  - **Denial of Service**
  - **Dictionary attacks**
  - **URL Interpretation**
  - **File Inclusion attacks**
  - **Man in the middle attacks**

- **System-based attacks**

- These are the attacks which are intended to compromise a computer or a computer network
- Some of the important system-based attacks are
  - **Virus**
  - **Worm**
  - **Trojan horse**
  - **Backdoors**
  - **Bots**

TYPES OF ACCESS ATTACK



Access Attack Types

Attacks on Secret Code

Phishing

Utilization of Trust Port

Social Engineering

Port Redirection

Man-in-the-Middle Attack

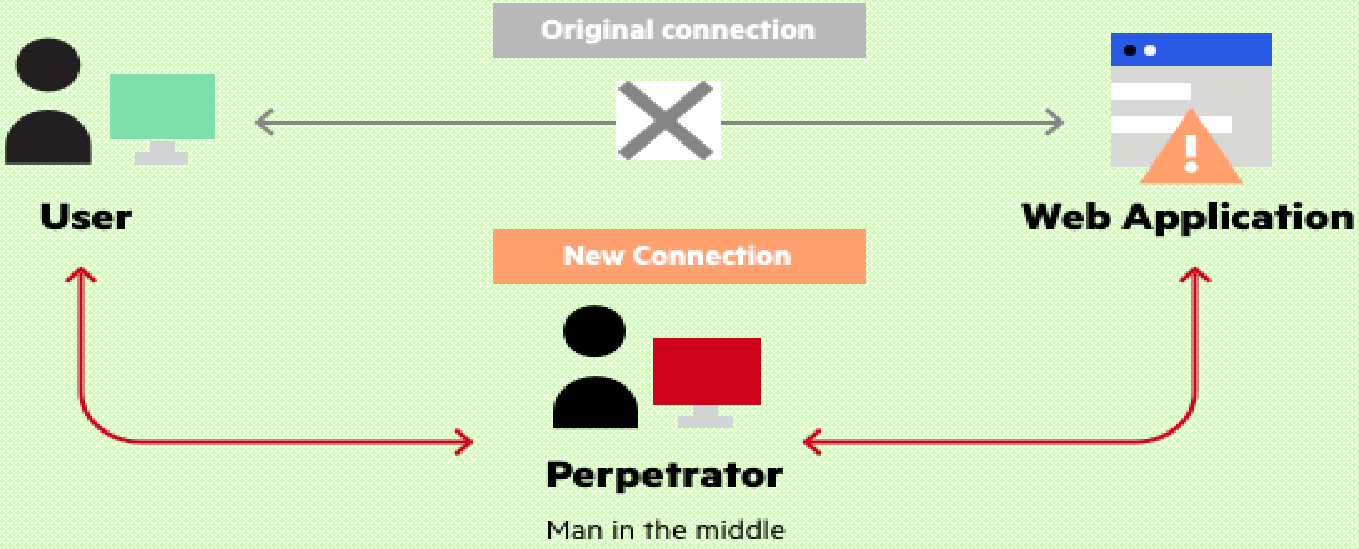
TYPES OF ACCESS ATTACK

- **Attacks on Secret Code:** A user without access or authority tries to hack into the account by utilizing every possible combination of passwords in a niche domain. This attack is also known as ***Dictionary Attack*** and usually occurs in two forms such as guessing of password and resetting of password
- **Utilization of Trust Port:** A trusted host is compromised by another trusted host by an unauthorized attacker to stage attacks
- **Port Redirection:** A hacker takes advantage of an established host to gain access to other hosts that are protected through network firewall
- **Phishing:** The action of pretending to be a licensed venture and sending fake e-mails to fool users into giving up private information that may be used for theft of identity

TYPES OF ACCESS ATTACK

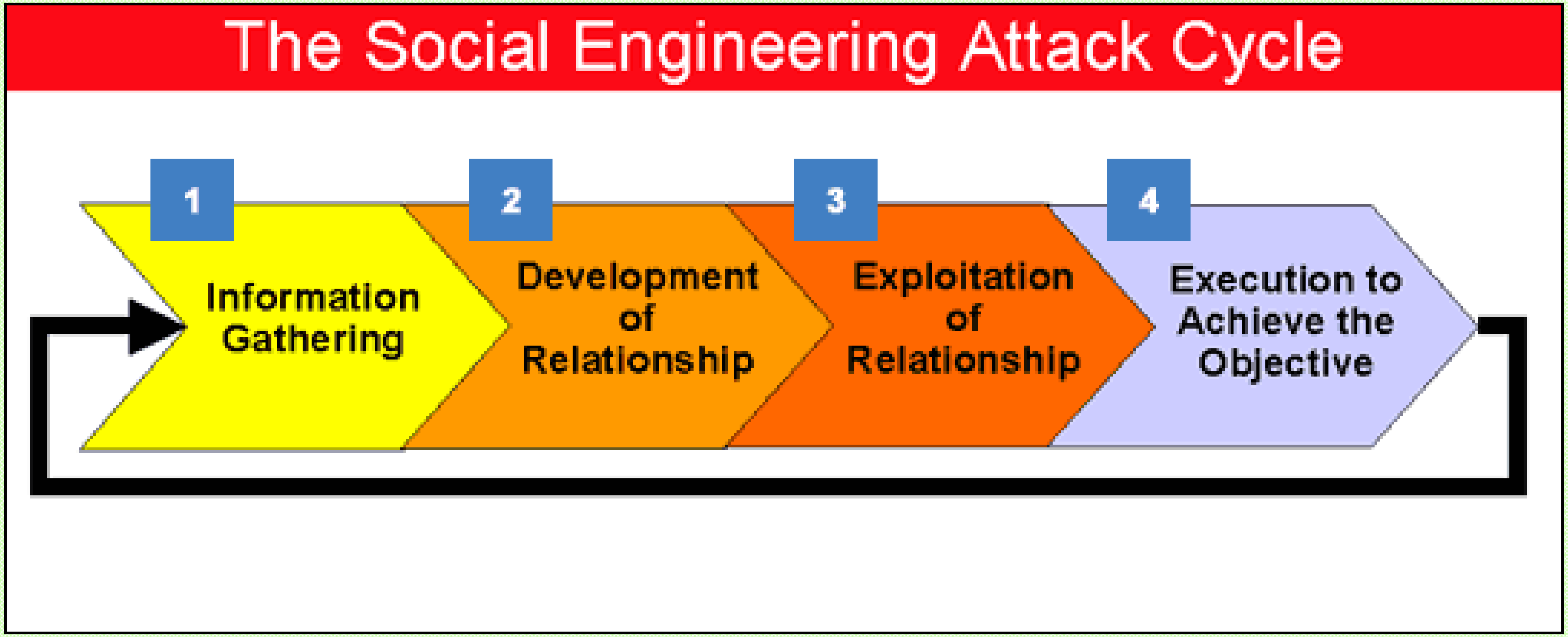
- **Man-in-the-middle Attacks:** Its an active eavesdrop attack where the attacker independently connects with the victim and relays messages between them

  This type of attack is also known as **Janus attack or bucket-brigade attack** makes the users to assume that the contact between them is private



TYPES OF ACCESS ATTACK

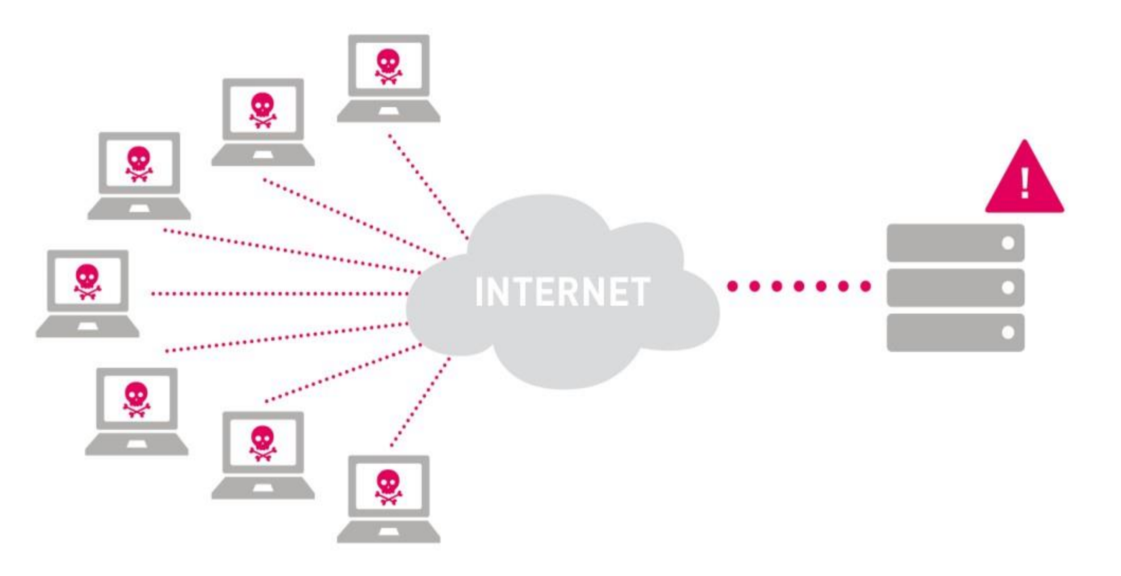
- **Social Engineering:** Malicious code infects social engineering websites through SQL injection leading to any users accessing the website and the contents to become infected and altered


The Social Engineering Attack Cycle
1
Information Gathering
2
Development of Relationship
3
Exploitation of Relationship
4
Execution to Achieve the Objective

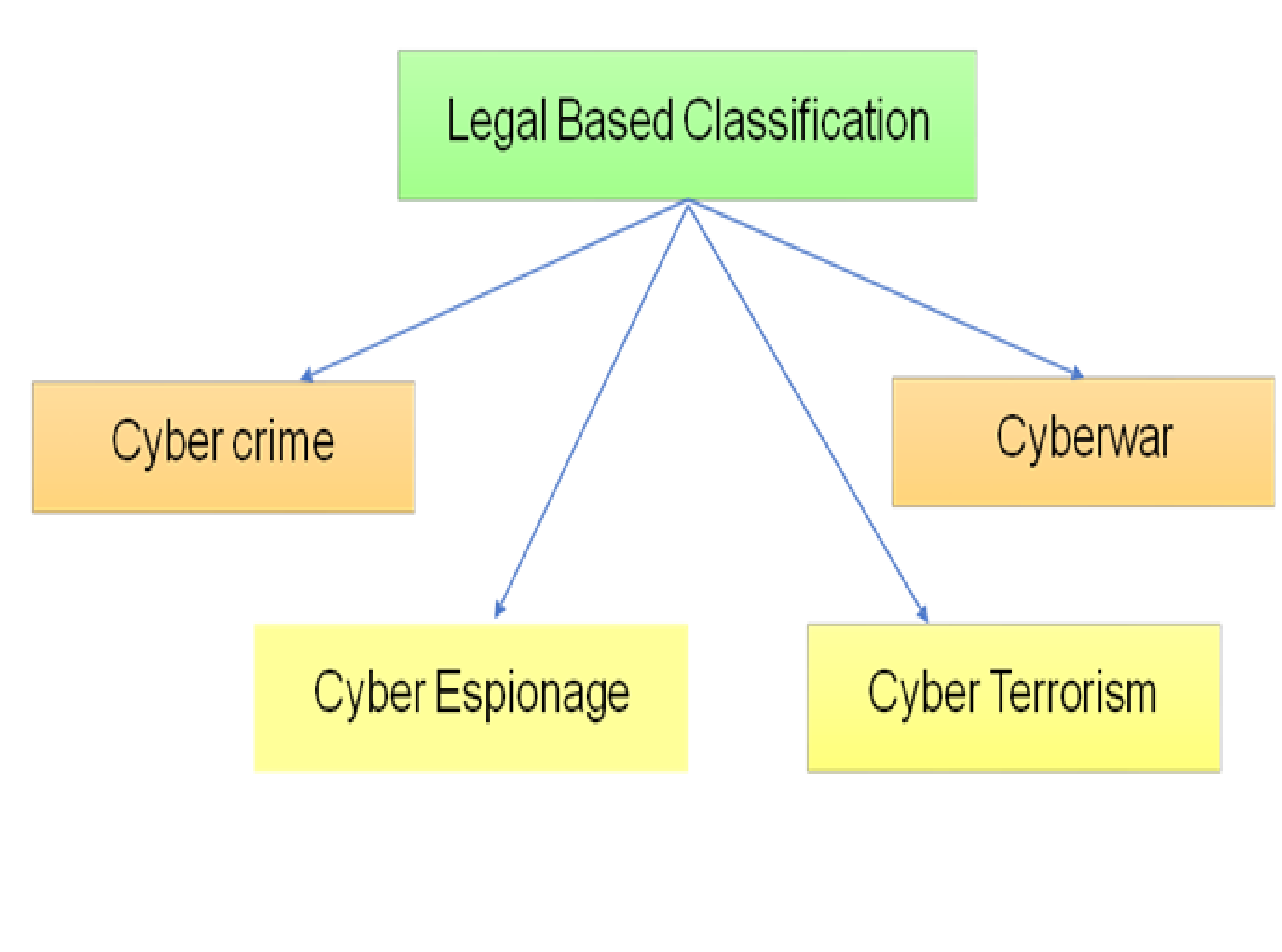
BASED ON PURPOSE

iii. Denial of Service Attack (DOS)

- It is the process of slowing down or crashing the system to render it slow or unusable
- It corrupts or delete the data/information and disables the network system by declining services to known users



LEGAL CLASSIFICATION



Legal Based Classification

Cyber crime

Cyberwar

Cyber Espionage

Cyber Terrorism

LEGAL CLASSIFICATION

- **Cyber Crime**

- Cybercrime is defined by Canadian law as,

  “A criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence”

- The objective is to use the system **as a tool to commit crime** and the computer as an auxiliary of the crime

- It occur due to the computer vulnerabilities includes,

  - **Operating System**
  - **Lack of user awareness**
  - **Anonymous nature and**
  - **Storage capacity**

LEGAL CLASSIFICATION

- **Cyber Espionage/Spying**

- The act of using malwares to obtain secret data of groups, individuals and governments to gain benefits through illegal means without any user authorization
- It is alternatively known as **cyber spying** and maybe completely carried out from computers in far away locations
- It possibly involves invasion at home by spies trained in computer usage or may be perpetuated by malicious amateur hackers and software programmers

LEGAL CLASSIFICATION

- **Cyber Terrorism**

- It is the activity carried out by terrorist on the Internet to disrupt large number of system networks with the means of computer virus

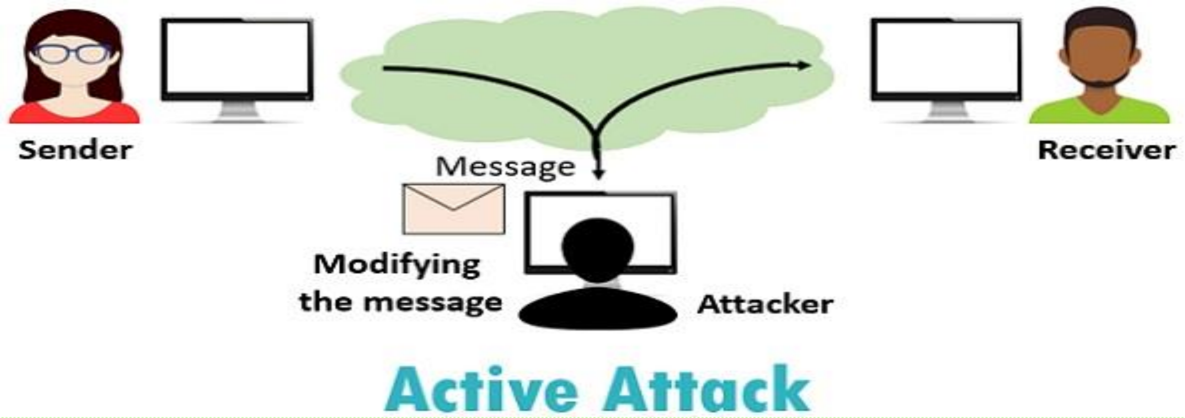
- **Cyber War**

- The act of attacking another Nation’s Computer or Network to cause disruption or disturbance

BASED ON SEVERITY OF INVOLVEMENT

- **Active attacks**

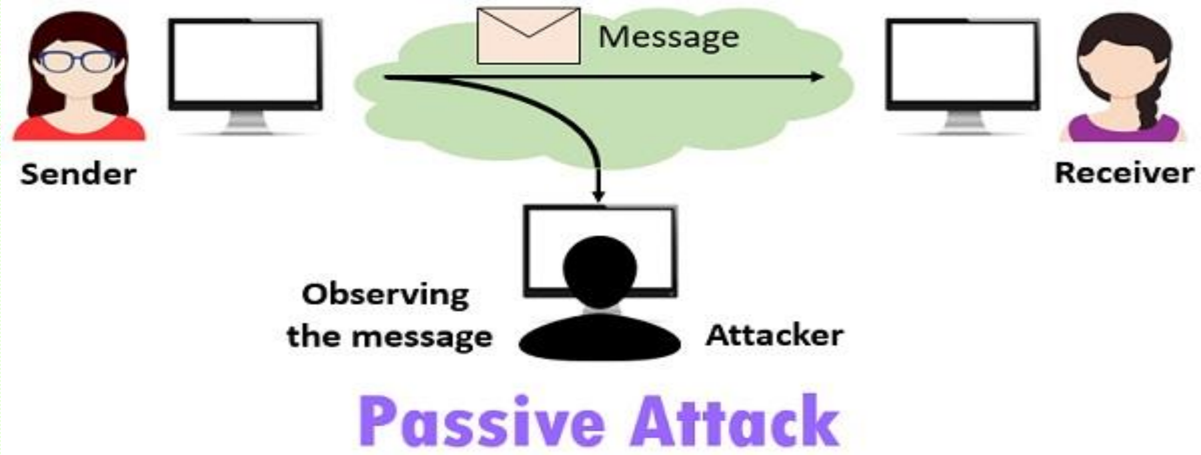
- It enables the attacker to communicate data to all the divisions or blocks data transmission in unidirectional or multidirectional communication
- The attacker located between the intercommunicating parties tries to terminate the data sent by the parties in the network
- As the server cannot authenticate the data source without validating the received information, the attacker replaces the client during this authentication process



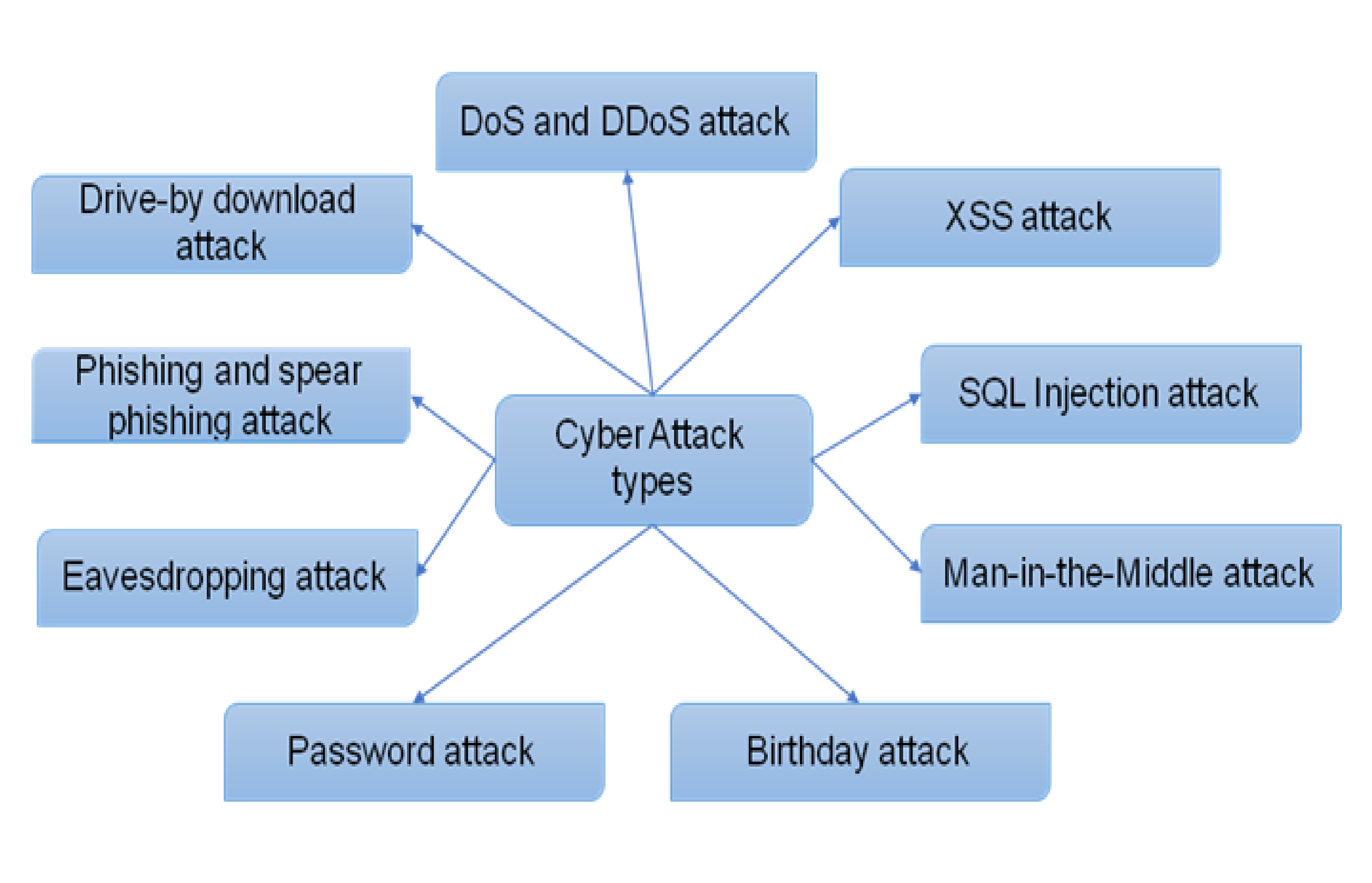
BASED ON SEVERITY OF INVOLVEMENT

➢ **Passive attacks**

- Using wiretapping or other similar methods, an unauthorized attacker spies to steal system information during the communication process that takes place between two parties
- This is different from an active attack as it does not interfere with any database but may still be considered a criminal offence



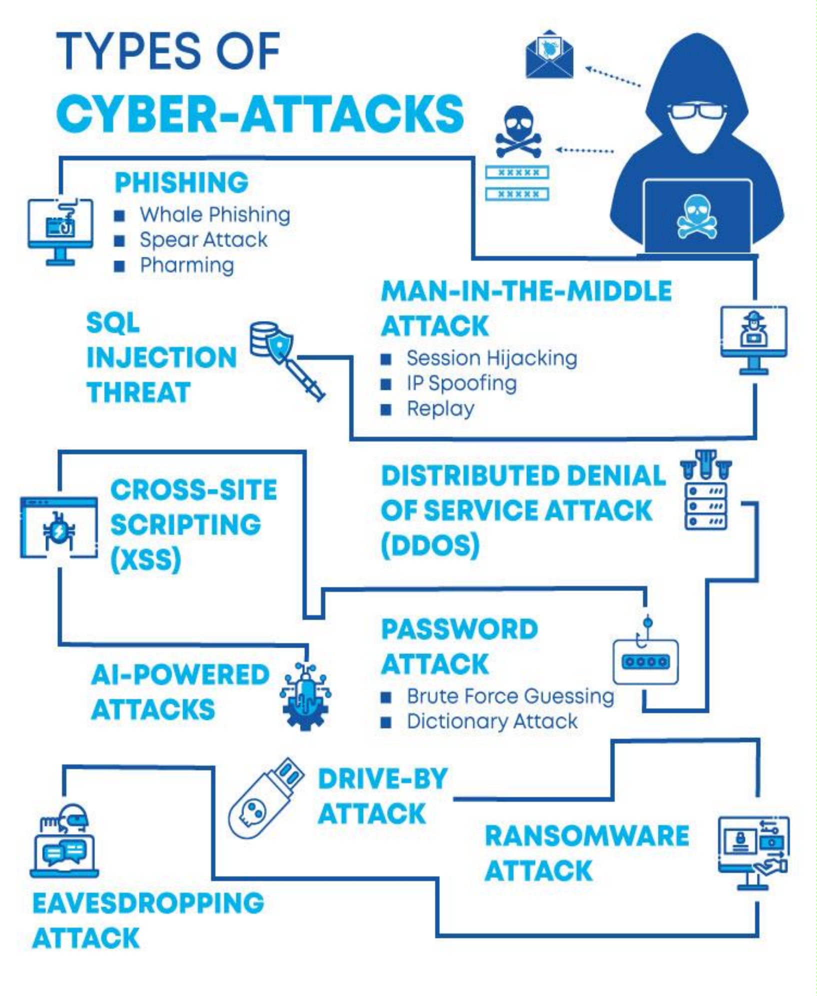
MOST COMMON TYPES OF CYBER ATTACKS



TYPICAL CYBER-ATTACK TYPES

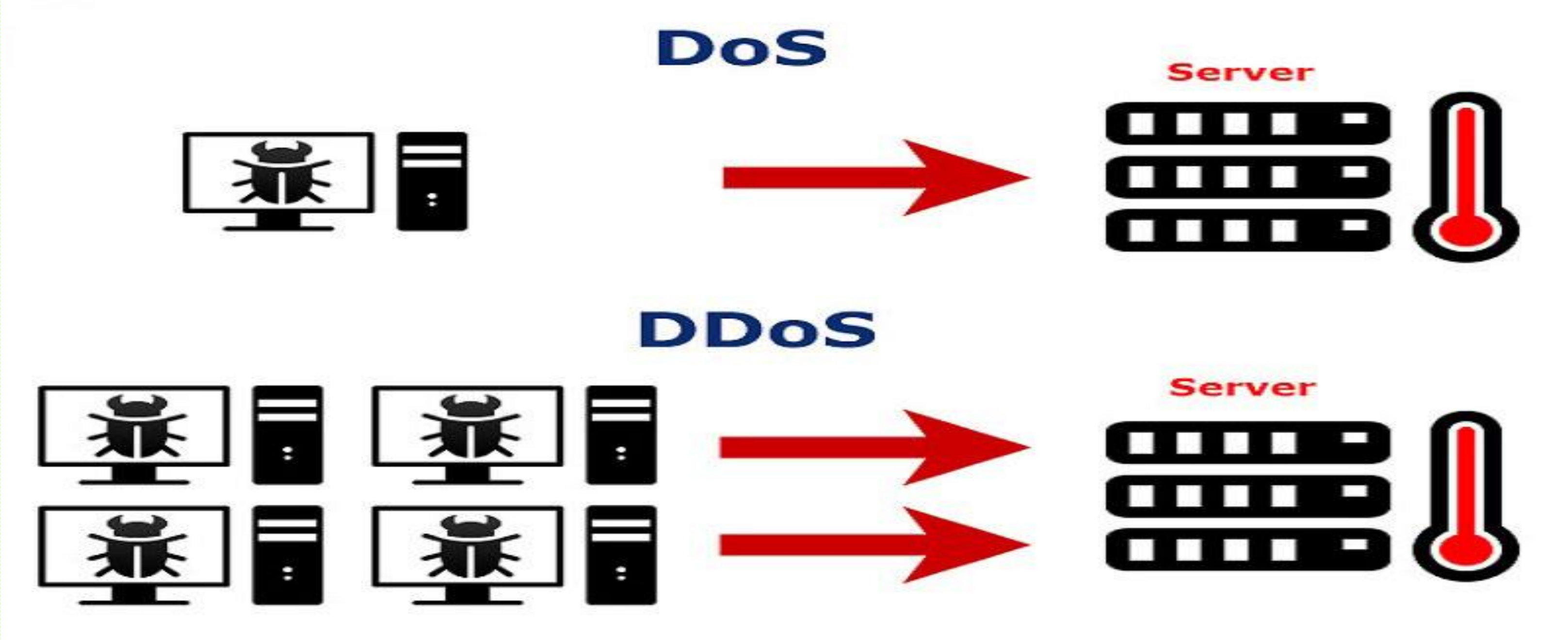
The most common types of cyber-attacks are listed below :

- DoS and DDoS
- XSS attack
- SQL injection attack
- Man-in-the-middle attack
- Birthday attack
- Password attack
- Eavesdropping attack
- Phishing and spear phishing
- Drive-by download attack



- **DoS Attack (Denial of Service Attack) and DDoS Attack (Distributed Denial of Service Attack)**

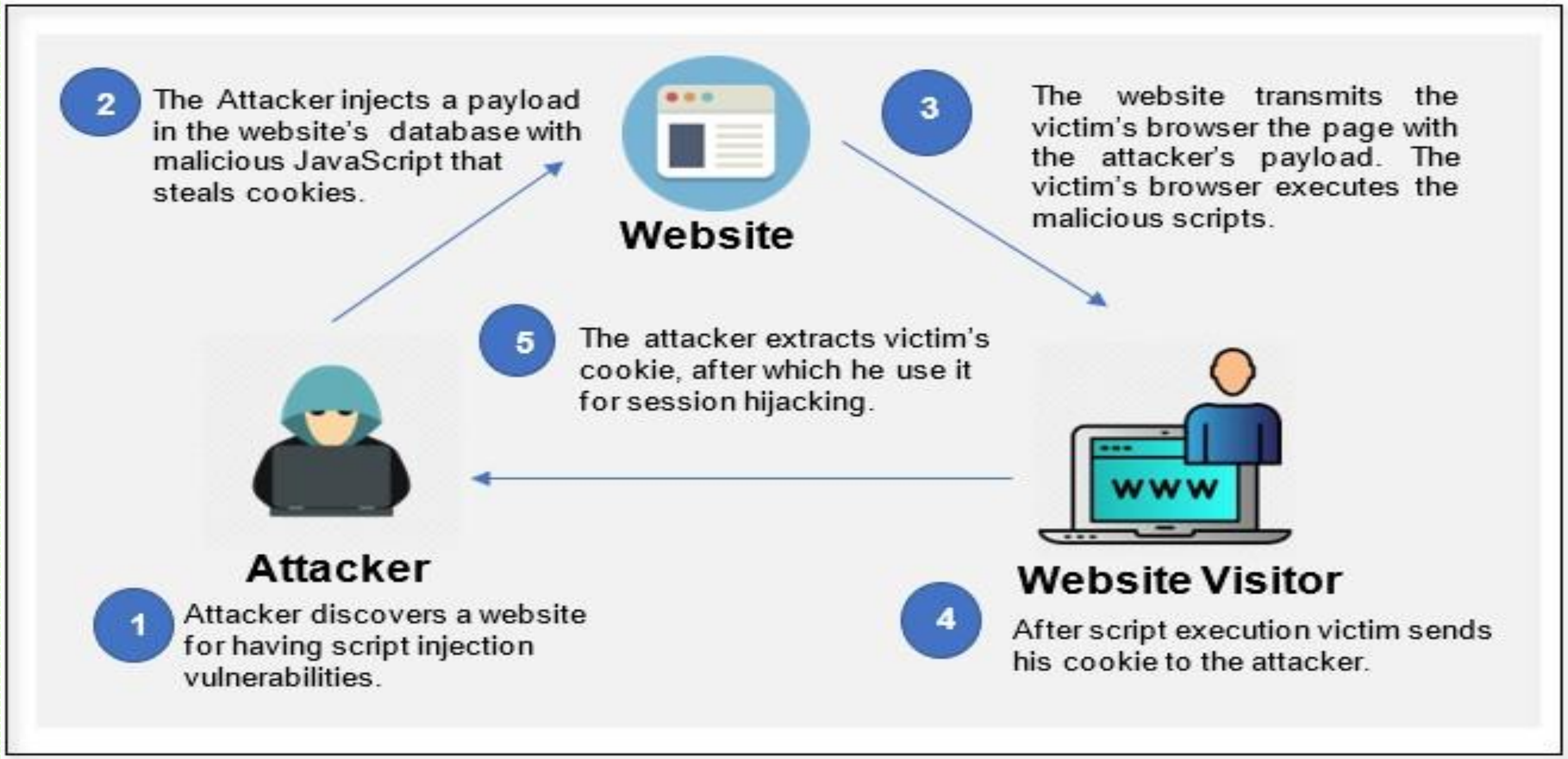
- DOS attack will make the system not to respond to the actual service requests by overpowering the system resources
- Distributed Denial of service attack is also similar to the DoS attack, but the difference is that the attack is launched from a series of host machines



- **Cross-site scripting attack (XSS Attack)**

- Using a third-party web resources XSS attacks will run a script on to the victim’s browser and application exactly injects load with malicious JavaScript in to the website database
- The malicious script is executed to the user’s browser as a HTML form when the user requests the page from the website
- For example, user cookies might be sending to the hacker’s server which is later on extracted and used to control the entire session
- The risk lead to enable the hacker to access and steal the cookies, then log key strokes, capture screenshots, explore and collect the entire network information and even take control or access remotely the user machine
- JavaScript is maintained widely on the web contents
- XSS can easily take advantage over VBScript, ActiveX and Flash

- Users should be given access to disable client-side scripts
- They can change the special characters like >, <, &, ?,/ to their respective URL encoded or HTML equivalents
- Developers can clean the user data by validating, filtering or escaping before it is reflecting back to the user helps effectively protects against XSS attacks



1 Attacker discovers a website for having script injection vulnerabilities.

2 The Attacker injects a payload in the website's database with malicious JavaScript that steals cookies.

3 The website transmits the victim's browser the page with the attacker's payload. The victim's browser executes the malicious scripts.

4 After script execution victim sends his cookie to the attacker.

5 The attacker extracts victim's cookie, after which he use it for session hijacking.

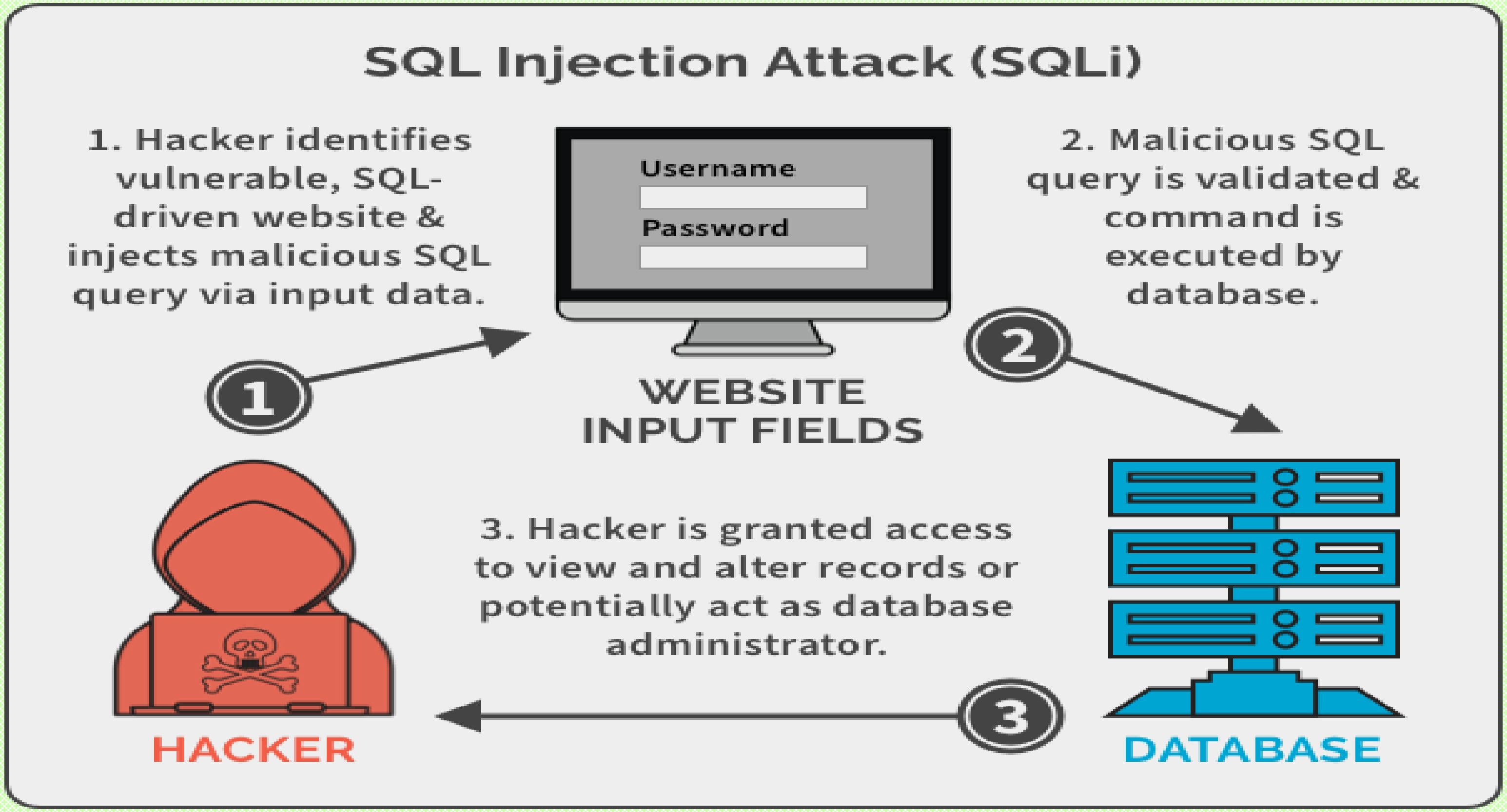
An example scenario of XSS Attack

➢ SQL injection attack

- In database-driven websites, one of the most common issues found is SQL injection attack
- It happens when the SQL query is executed to the database which is the input from the client and the server
- To run predefined SQL commands, instead of login and password the commands are placed in the data plane which reads sensitive data and modify the data by inserting irrelevant data
- Administration operations could be executed such as updating, deleting and shutdown on the database
- A particular form in the site may ask for user’s account name and sends to the database to user account number to get associated information. The dynamic query may look like,

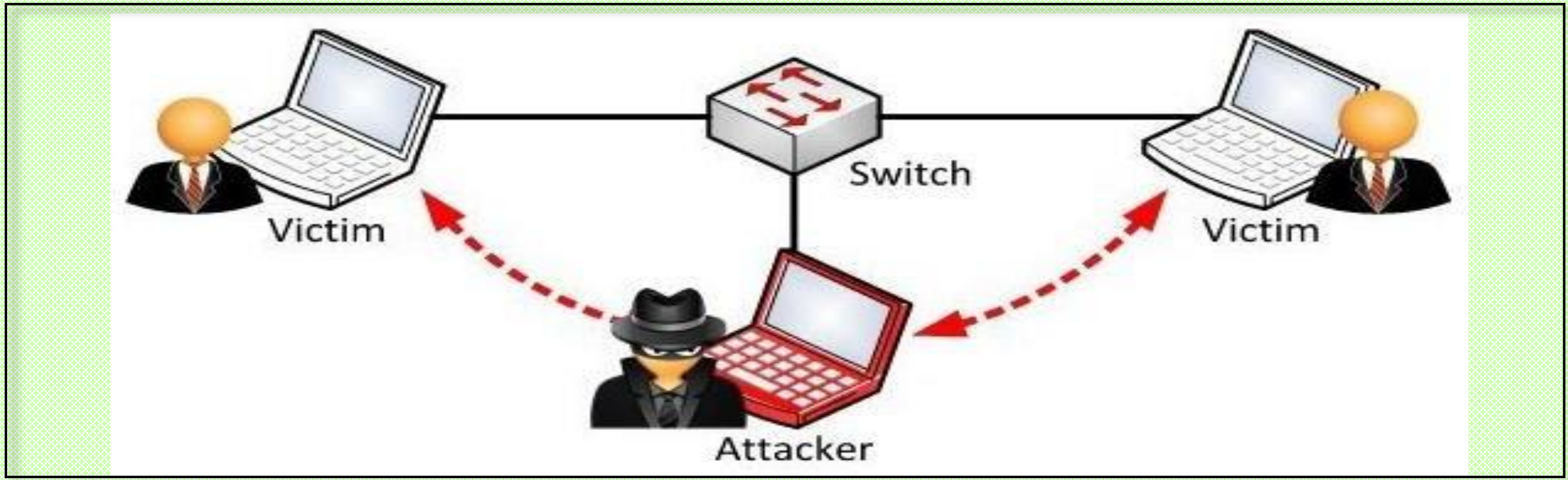
```
“SELECT * FROM users table WHERE accountNo = ‘“ +UserAcctNumber +”’;”
```

- SQL injections mostly work, if a website uses dynamic SQL
- SQL injections have been less likely to get exploit by the J2EE
- So, the queries and codes used in the database should be strong to prevent against this SQL Injection Attack


SQL Injection Attack (SQLi)
1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.
Username
Password
WEBSITE INPUT FIELDS
2. Malicious SQL query is validated & command is executed by database.
1
2
3
3. Hacker is granted access to view and alter records or potentially act as database administrator.
HACKER
DATABASE

➢ Man-in-the-middle attack (MITM Attack)

- Man-in-the-middle attack happens when a hacker inserts manipulates the traffic by being in between the client and server

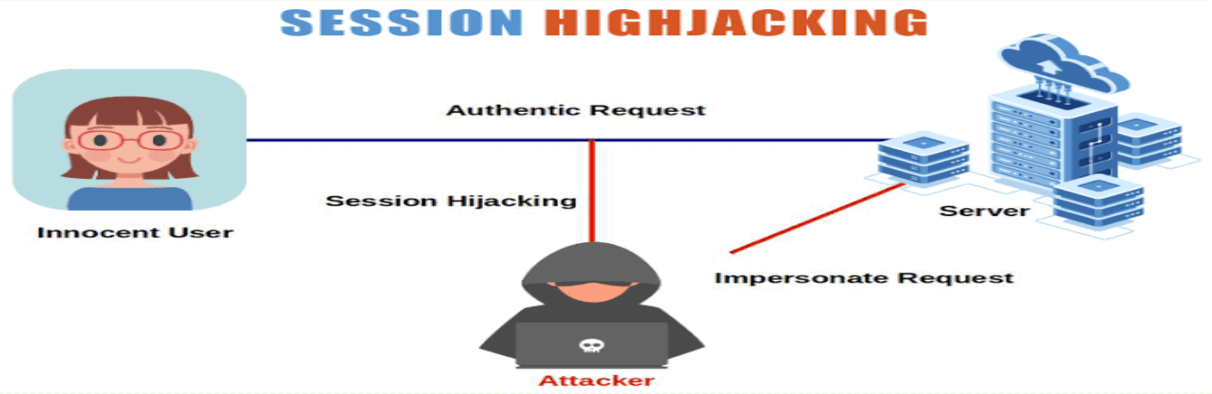


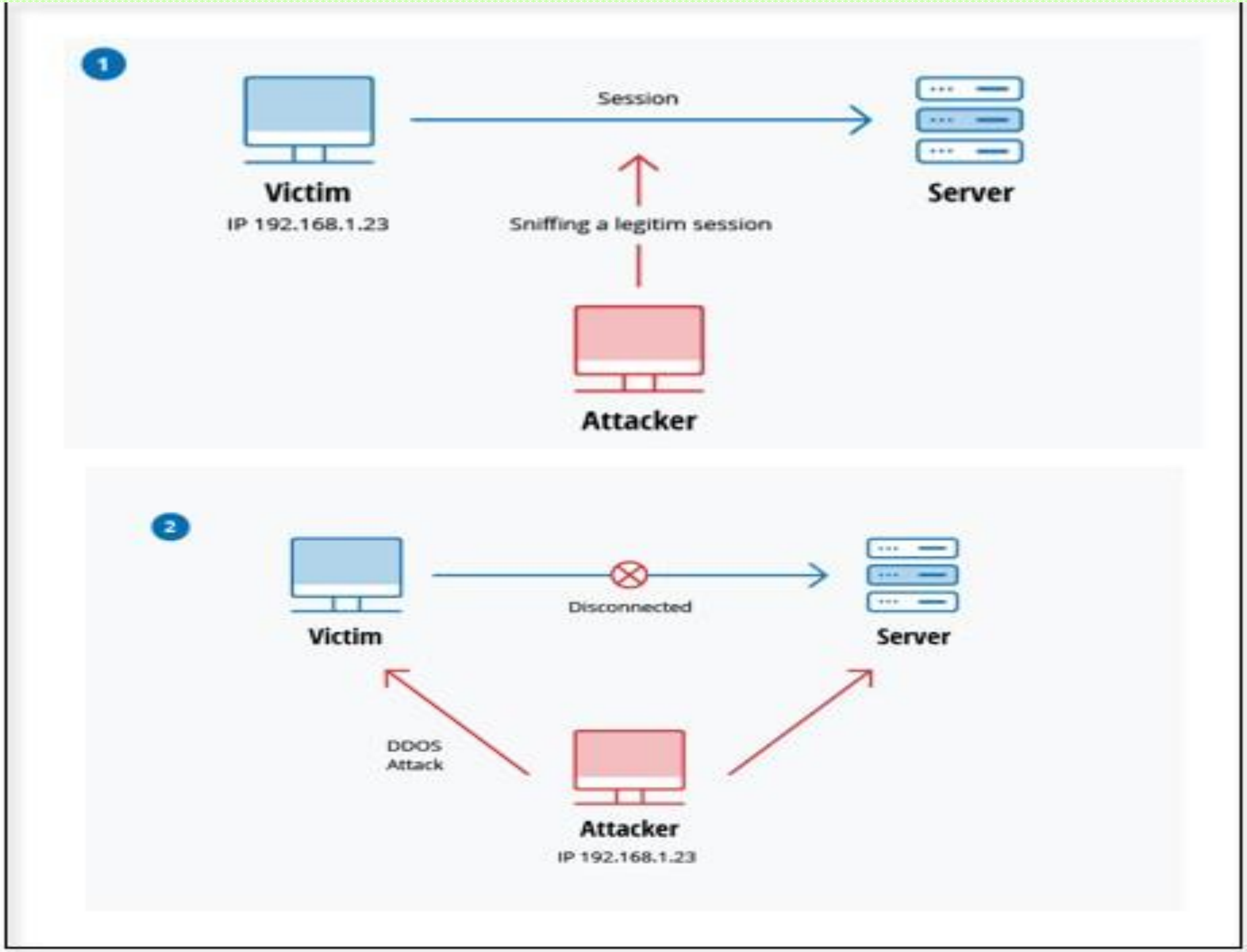
An Example of Man-in-the-Middle Attack

- The common types of these attacks are listed below:
  - **Session hijacking**
  - **IP spoofing**
  - **Replay attack**

➢ Session hijacking

- Session hijacking happens when a hacker hijacks the established connection between a client and server
- The attacker changes the IP address for a trusted client, making the computer believe it is communicating with the actual server
- **For example,**
- When a node tries to access the server, the attacker gains control and changes the Client’s address as its own address and communicates with the server

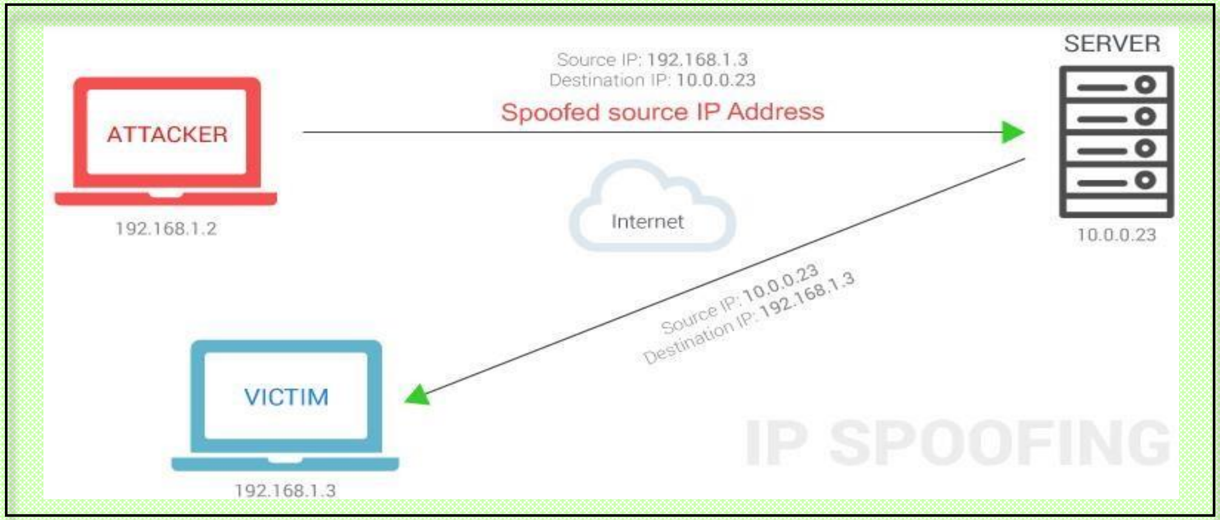




An example scenario for session hijacking attack

➢ IP Spoofing

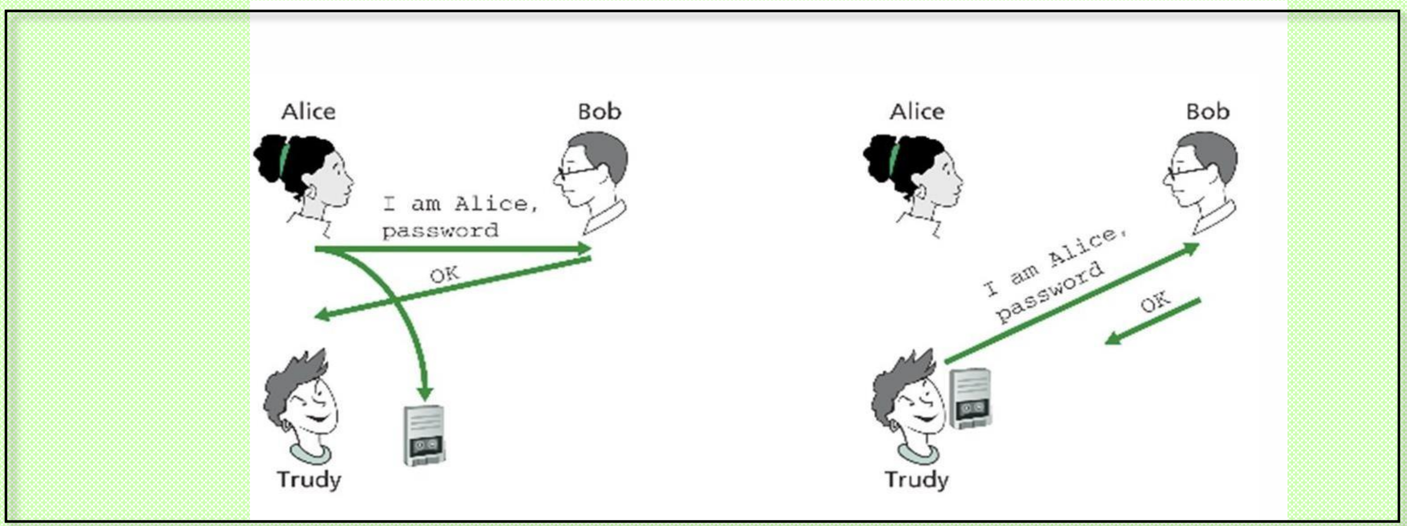
- IP spoofing is used to convince the victim that he or she is connected to a trusted and known entity, which results in the attacker gaining access to the system
- The attacker communicates with victims as if he/she knows the address to the user and makes the victim accept the packet and infect the user's system



An example for IP Spoofing Attack

➢ Replay Attack

- Also known as ***play back attack***, happens when a data transmission is hacked and purposely delayed or repeated, which gives the user the sense that the transaction is complete
- But the hacker can still access the server through the transaction initiated by the attacker
- Unless mitigating steps are taken, these kinds of attacks are repeated and the user or the victims generally assume that the transactions are legitimate
- Using digital signatures with timestamps can help to stop these kinds of Man in the middle attack
- Depending on the nature of the application, providing the option of one-time password can help stop unwanted eavesdropping when the client and server are in a session



An example of Replay Attack

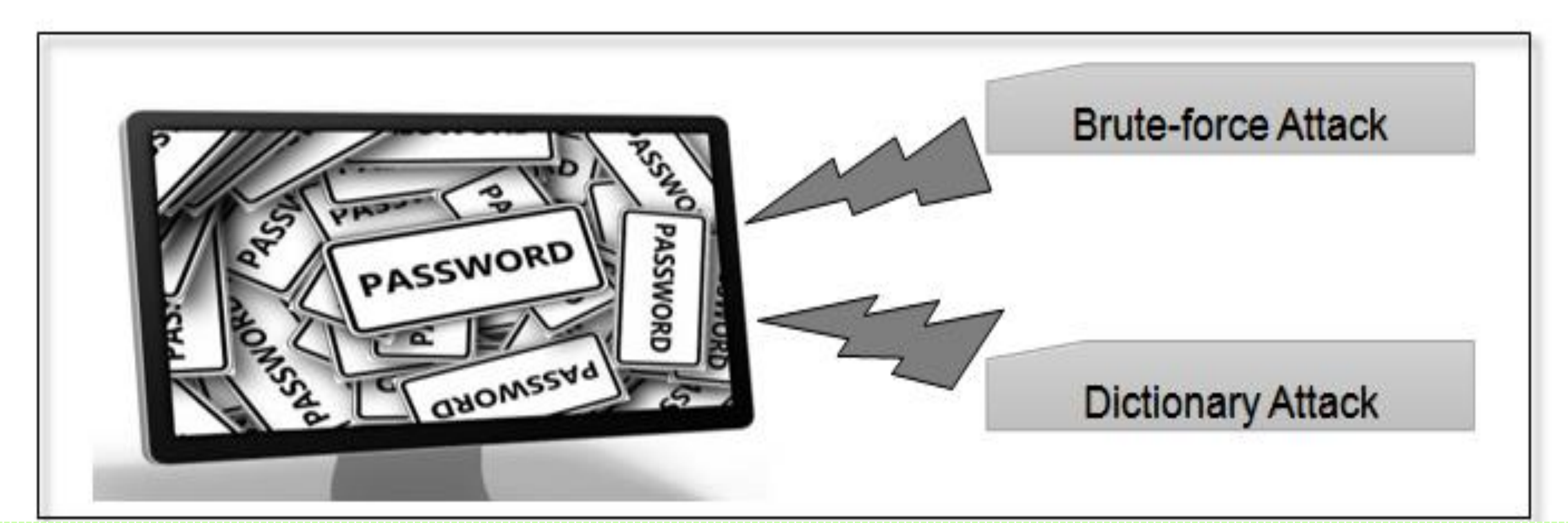
- In the given example, Trudy is the attacker who replays the conversation between Alice and Bob
- When Alice sends a message to Bob, Trudy being the MitM attacker interrupts the communication and replays the message to attack the Bob's system in the name of Alice.

➢ Birthday Attack

- The integrity of a message, software or digital signature is verified using the hash algorithms which are made against the birthday attacks
- Message Digest (MD) of fixed length is produced by the hash function and it uniquely characterizes the message and its length is independent
- When the hash function is processed, basically the birthday attack refers to the probability that two random messages generates have the same Message Digest
- The user messages are replaced with these messages
- The receiver here is not able to identify the replacement of the messages even if he/she tries to compare with the Message Digests (MDs)

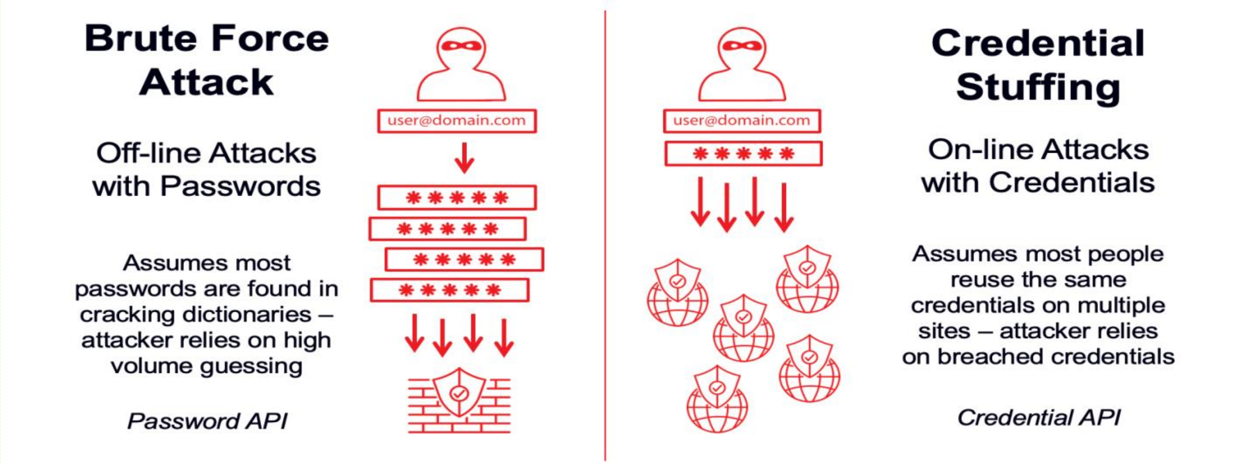
- **Password attack**

- Unauthorized access to the network to obtain unencrypted passwords, watching around the user desktop, taking access to the database or guessing both by a random or systematic manner are the common mechanisms to validate user's information system
- There are two methods applied to launch an effective password attack



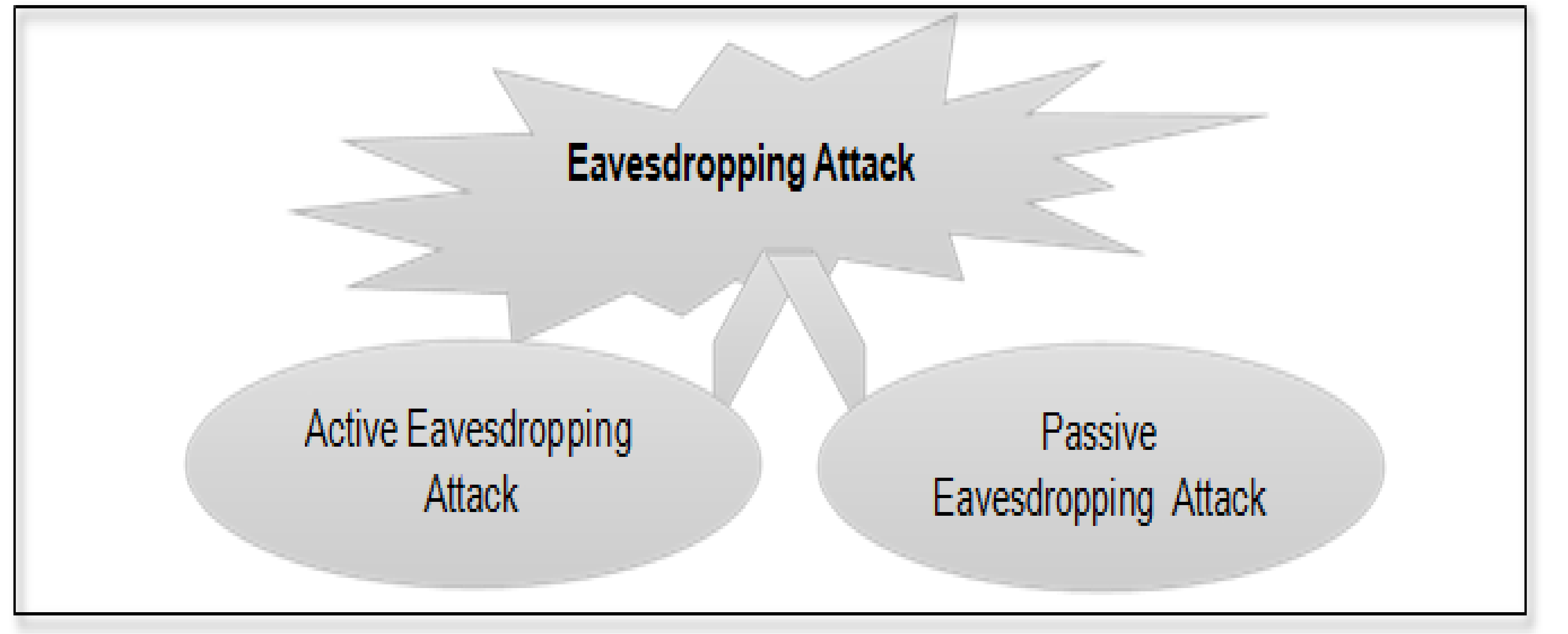
Types of Password Attacks

- **Brute-force** – It is a method by applying some logic guessing and trying password randomly related to a person’s name, job title, hobbies and more
- **Dictionary attack** – Hackers use this method by copying an encrypted file that holds password, the commonly used password dictionary is applied with the same encryption and the results are compared to gain access to a host or a network
- So, an account lockout policy which locks the account after three unsuccessful password attempts should be implemented to defend the host or a network from dictionary or brute force attacks


Brute Force Attack
Off-line Attacks with Passwords
Assumes most passwords are found in cracking dictionaries – attacker relies on high volume guessing
Password API
user@domain.com
*****
*****
*****
*****
user@domain.com
*****
Credential Stuffing
On-line Attacks with Credentials
Assumes most people reuse the same credentials on multiple sites – attacker relies on breached credentials
Credential API

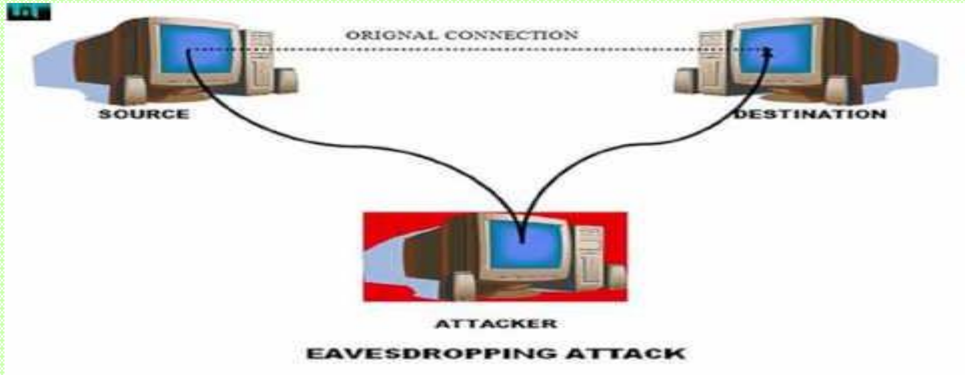
➢ Eavesdropping attack

- The user details like credit card numbers, passwords and their private information sent over the network are gained by the attacker in this attack
- This attack can be passive or active in nature and occurs through the interruption of network traffic.



Types of Eavesdropping Attack

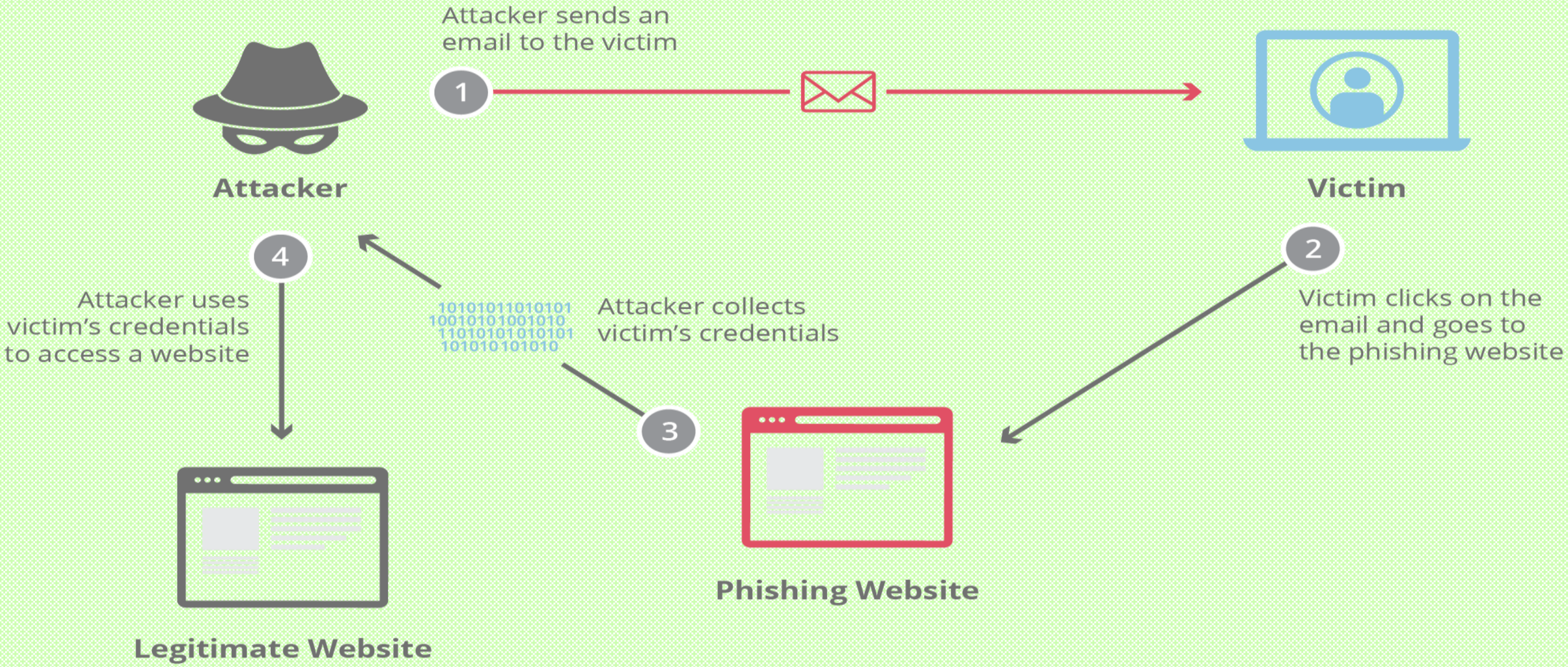
- **Passive Eavesdropping** – User information hacked by spying the transmission of a message in the network by a hacker
- **Active Eavesdropping** – This is also named as probing, scanning or tampering. Hacker acts as a friendly unit by concealing himself can grab information actively and send queries to the transmitters.
- Passive eavesdropping detection is more important that active eavesdropping because by conducting passive attack the attacker gains information of the neighbor units in active attacks
- Encryption of data is the best and one of the security measures in eavesdropping attack

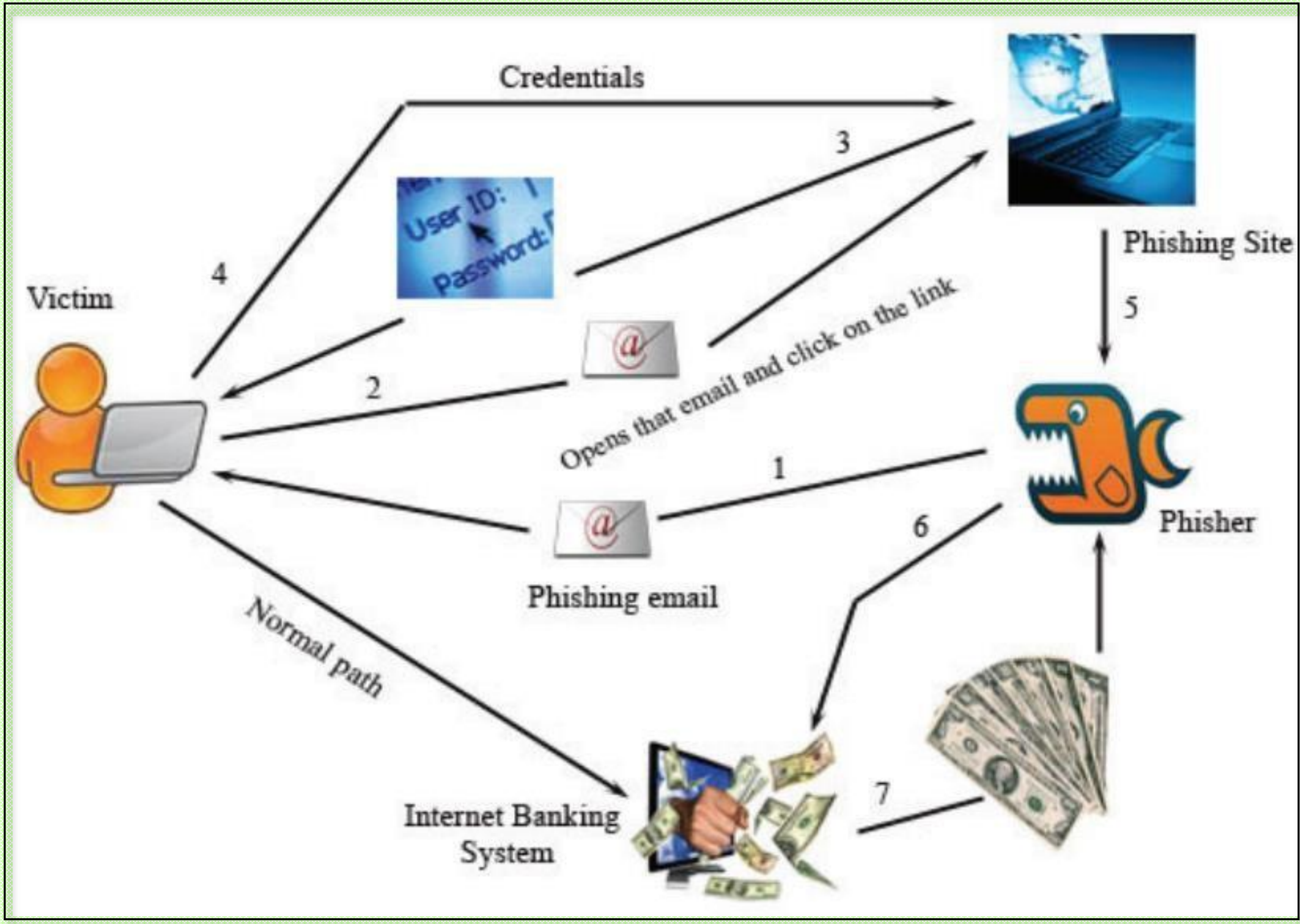


Phishing and Spear Phishing attacks

- Sending an email which can look from trusted sources but actually is from a attacker is known as **phishing**
- Phishing is carried out to trick the user to give out personal information or sensitive material that the attacker seeks or making the user to visit a potentially malicious page
- These type of attack can come under social engineering
- Phishing attack is targeted towards a wide range of users and emails are chosen at random
- When a phishing attack is conducted on a targeted audience this is generally known as **spear phishing**

- **The following steps can be taken to avoid phishing attacks**:
  - ➢ It is important to analyze an email before following a link
  - ➢ Checking the source of the email is always important if it requests for any data or asks the user to download a document
  - ➢ Hovering over the link will reveal the actual address of the webpage which can help the user identify potential attack

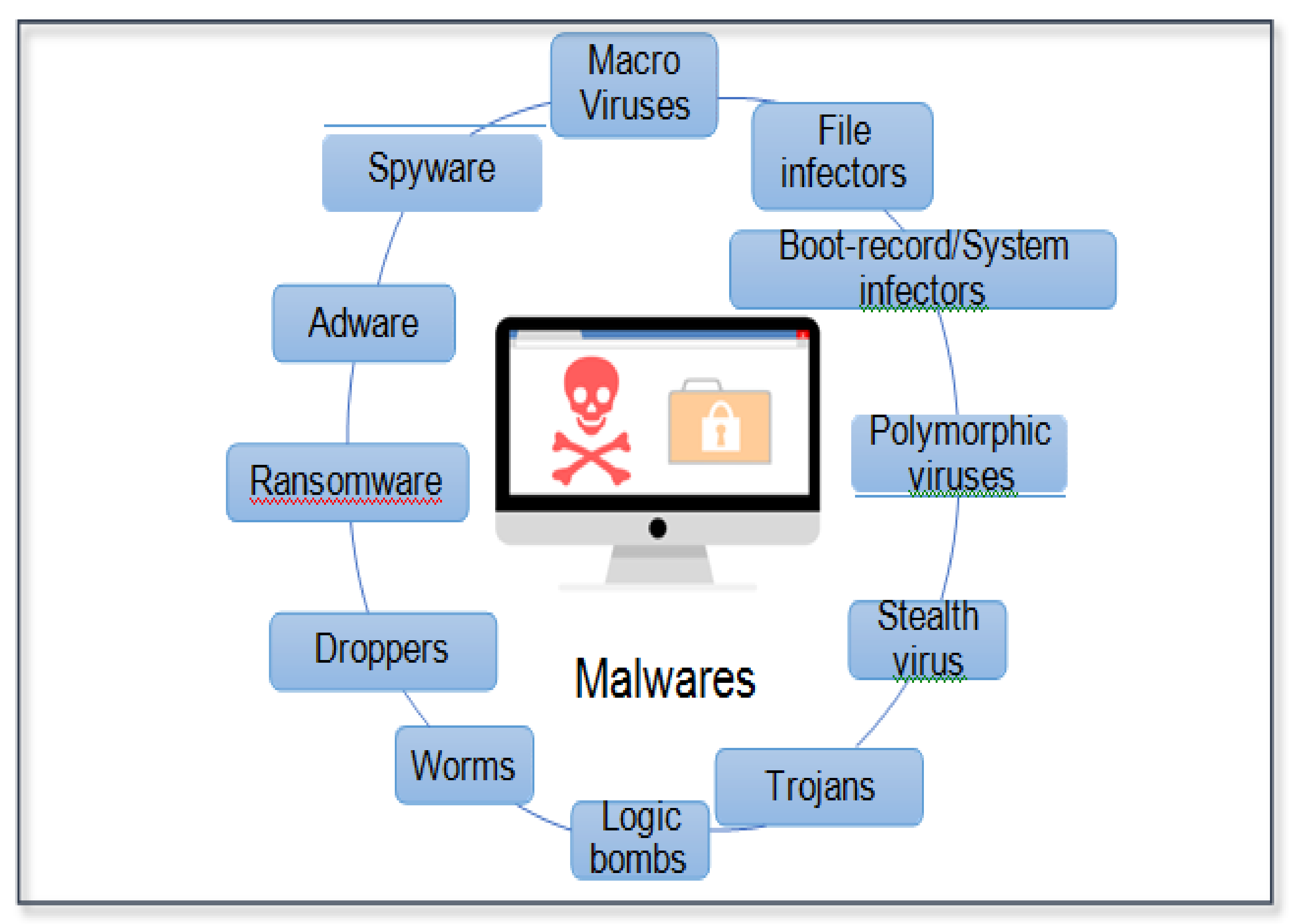

Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
10101011010101
10010101001010
11010101010101
101010101010
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website



An example scenario of Phishing Attack

MALWARE ATTACKS

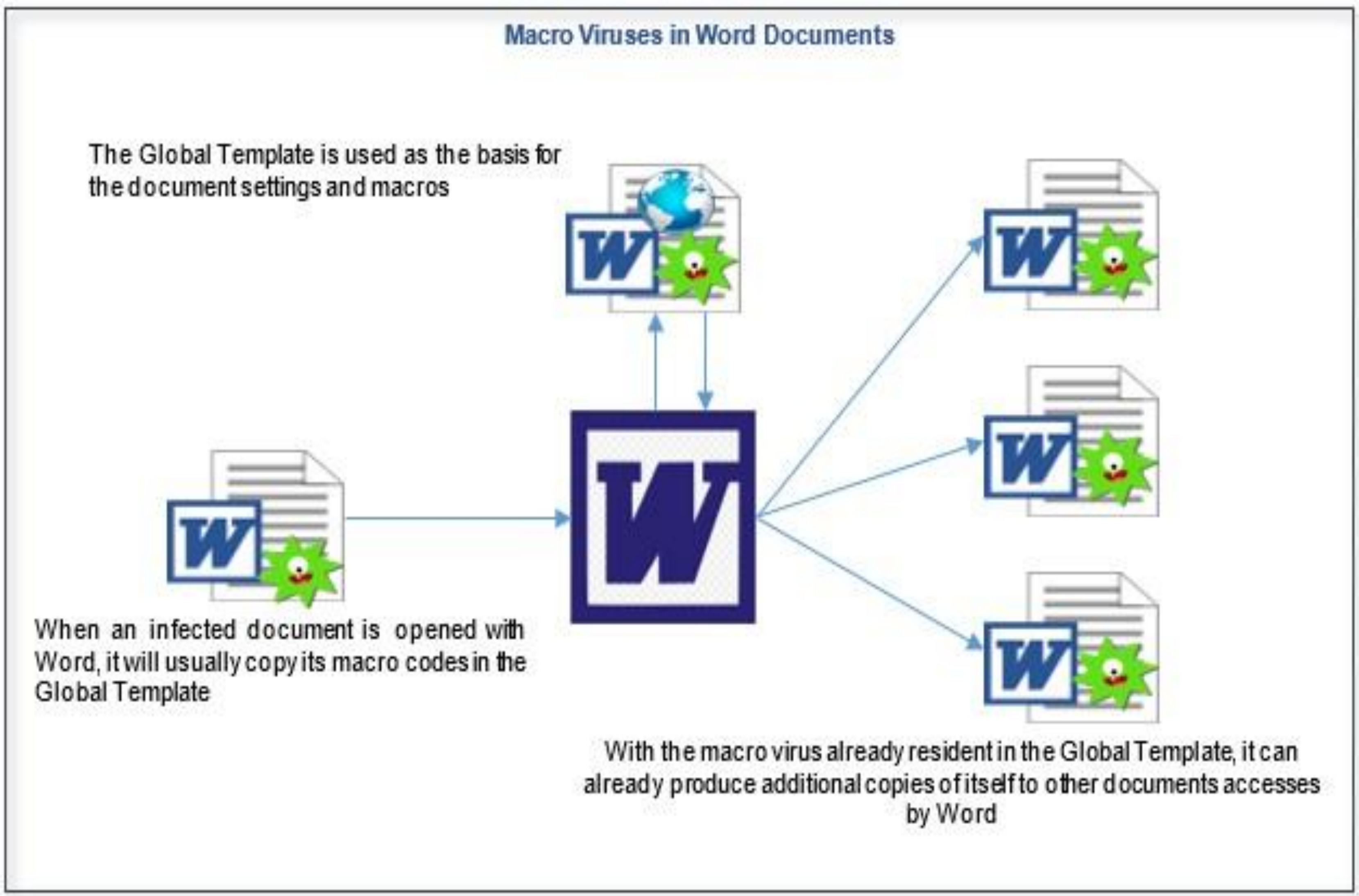
- Malware is otherwise known as **malicious software or unwanted software** that is installed in the system without the knowledge of the user
- A genuine code is attached with the malicious program and broadcasted.
- It duplicates itself in the global network i.e., Internet



Different types of Malwares

- **Macro Viruses**

- Earlier versions of Microsoft applications such as excel, word and power point are infected by this Macro Viruses
- This virus is attached to the application and initializes sequences
- Whenever the application is started, the control initially transferred to the virus which executes the instruction
- It transfers control before the execution of the application and here it duplicates itself and adds to the other available code in the entire system



Macro Viruses in Word Documents

The Global Template is used as the basis for the document settings and macros

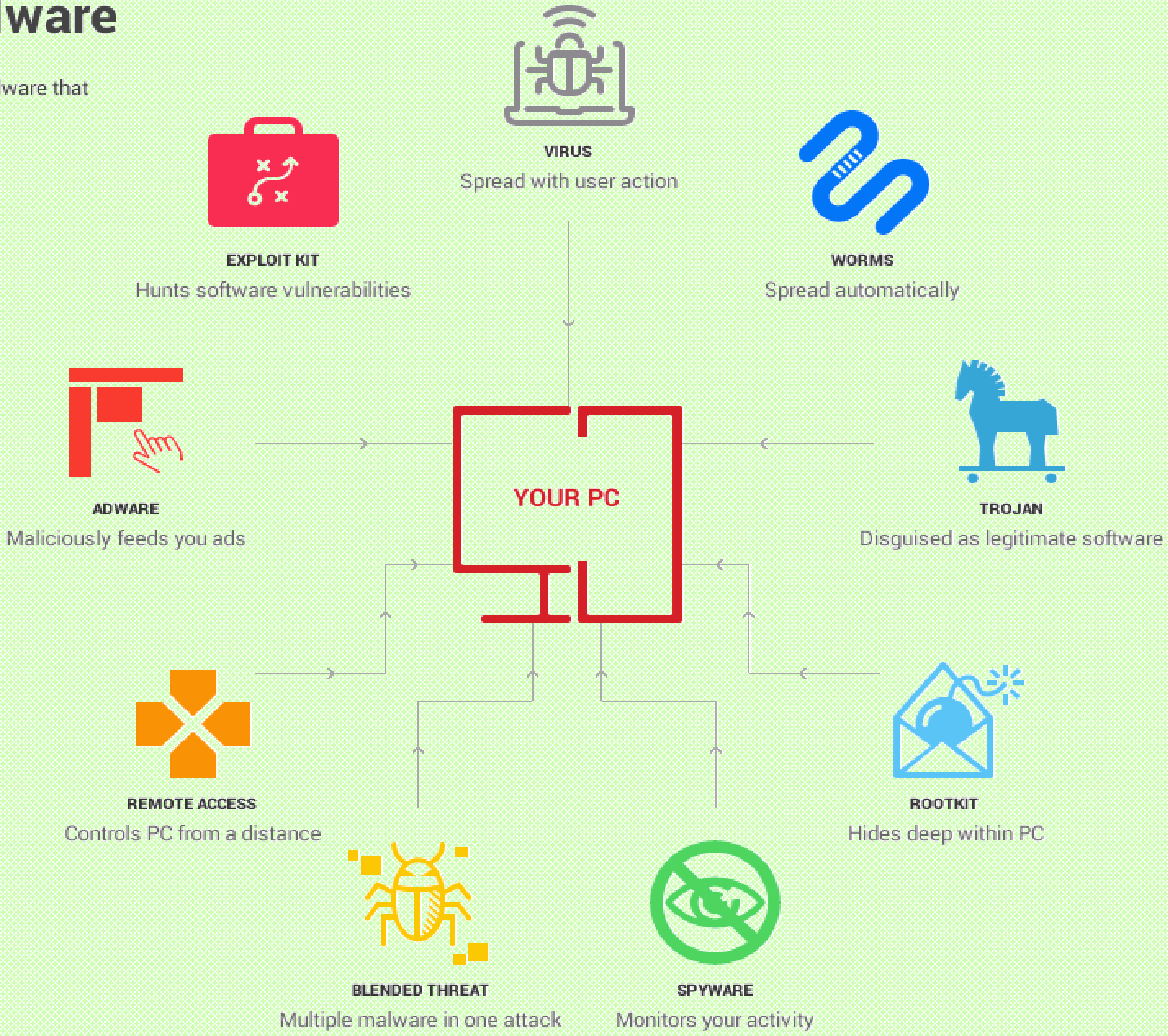
When an infected document is opened with Word, it will usually copy its macro codes in the Global Template

With the macro virus already resident in the Global Template, it can already produce additional copies of itself to other documents accesses by Word

An example of Macro viruses in Word documents

Types of malware

These are the main types of malware that can be found across the web.



VIRUS
Spread with user action

EXPLOIT KIT
Hunts software vulnerabilities

WORMS
Spread automatically

ADWARE
Maliciously feeds you ads

YOUR PC

TROJAN
Disguised as legitimate software

REMOTE ACCESS
Controls PC from a distance

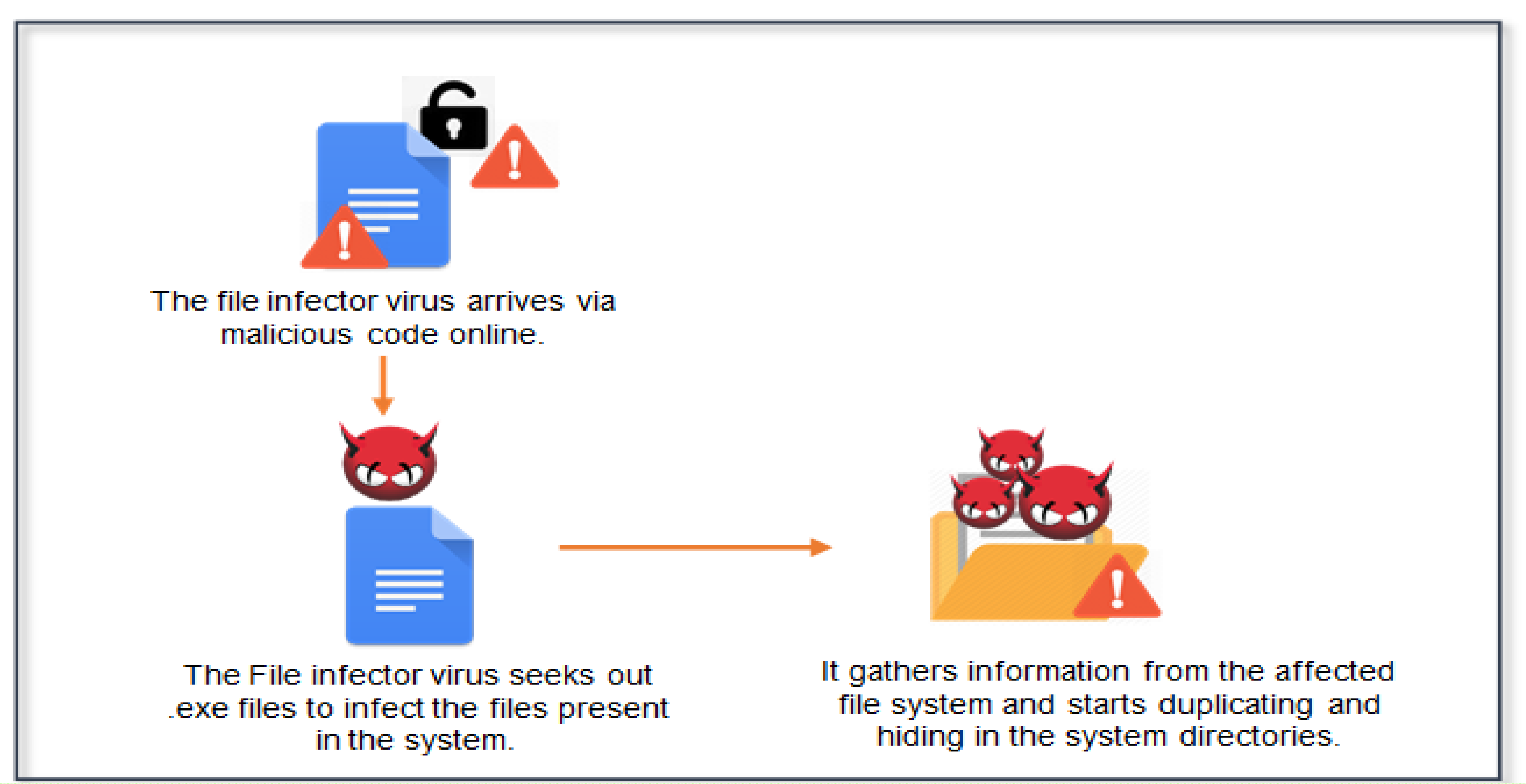
ROOTKIT
Hides deep within PC

BLENDED THREAT
Multiple malware in one attack

SPYWARE
Monitors your activity

- **File Infectors**

- This type of viruses basically is attached to executable code such as exe files
- Whenever the exe file loads the code the virus is installed



The file infector virus arrives via malicious code online.

The File infector virus seeks out .exe files to infect the files present in the system.

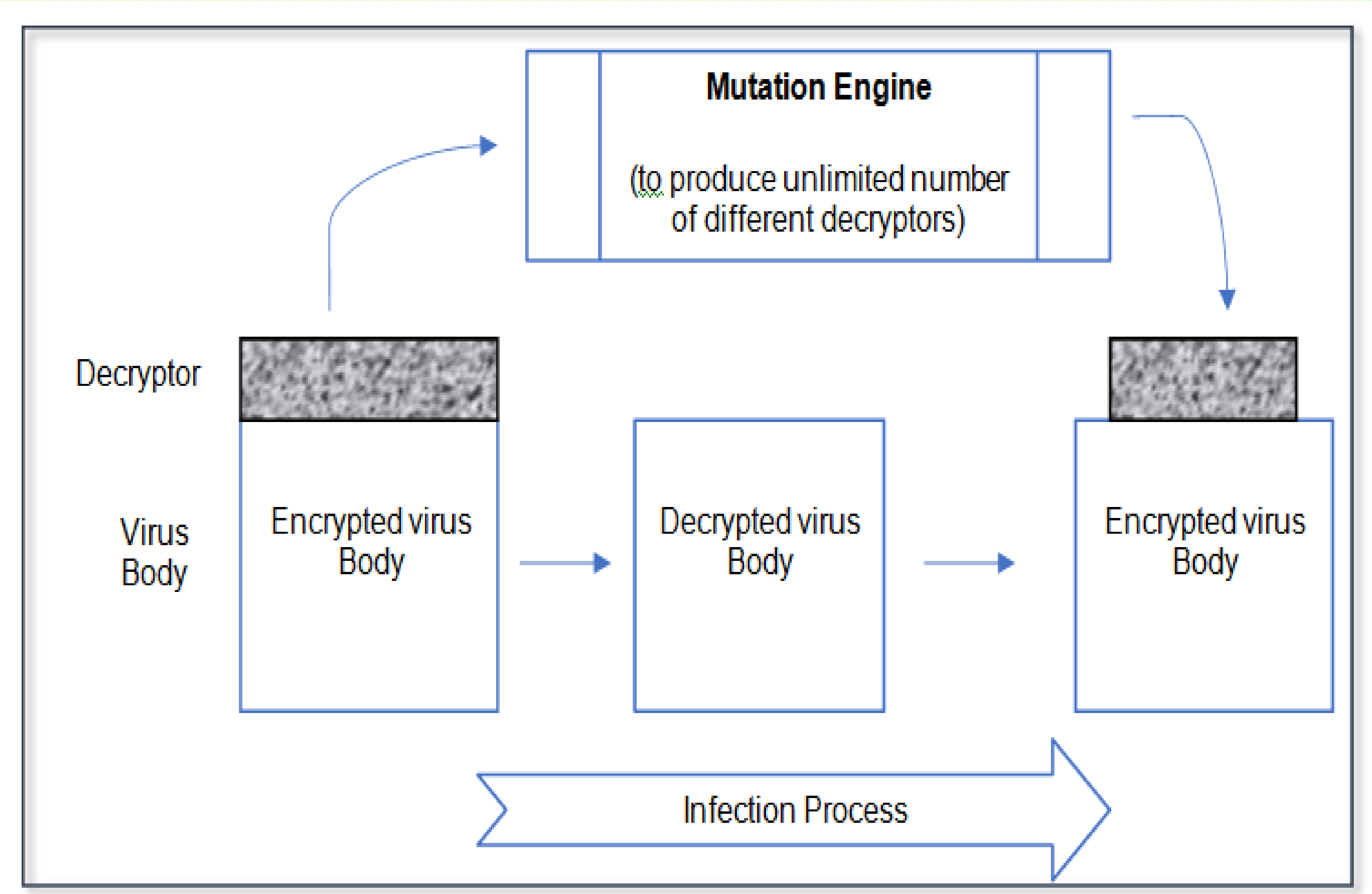
It gathers information from the affected file system and starts duplicating and hiding in the system directories.

An example of File infector virus

- **Boot-record/System infectors**
- In the case of system or boot record infectors, the virus is added to the hard disks in the master boot record
- The virus is loaded in the memory from the master boot record when the system is started
- Other disks and computers are infected by this virus
- **Stealth viruses**
- It takes over the system functions to hide in it, so that it compromises the malware detection software not to display them in the detected list
- Infected area is shown as uninfected in the report.
- This type of viruses changes to the latest modified date and time of the file or hides the details about the infected file size

- **Polymorphic Viruses**

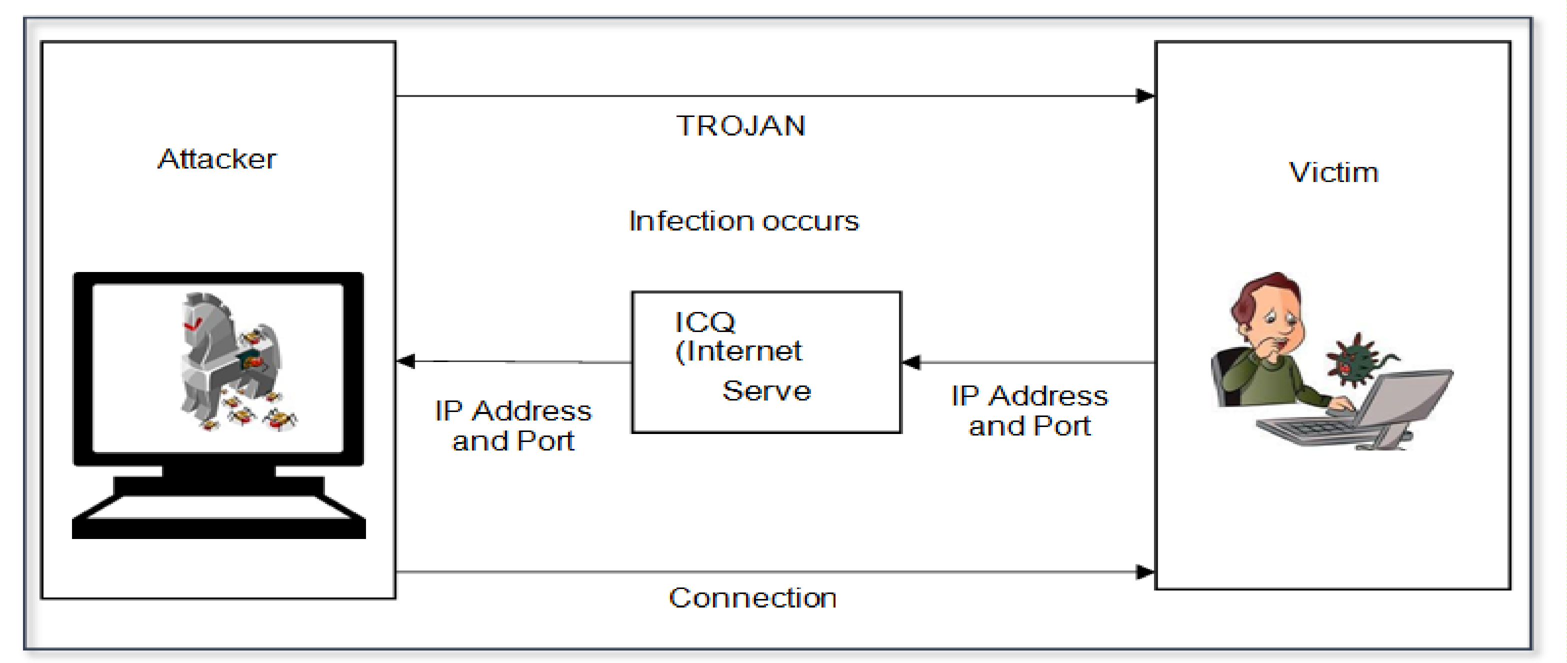
- These viruses hide themselves in various cycles of encryption and decryption
- A new decryption routine is developed by the mutation engine
- By using an algorithm corresponding to the new developed decryption code, the mutation engine is encrypted by the virus
- The encrypted package of mutation engine and the virus are added to new code and this process is repeated, such viruses are very difficult to detect
- Since it has many modifications of the source code these viruses have the high level of entropy
- Tools like Process Hacker or Antivirus software can use this feature to detect them



An example of Polymorphic Virus

➢ Trojans

- A malicious function which hides in a useful program is known as ***Trojan or Trojan horse.***
- Unlike viruses it does not self-replicate
- Trojans establish a back door that can be exploited by the attackers in addition to launching attacks

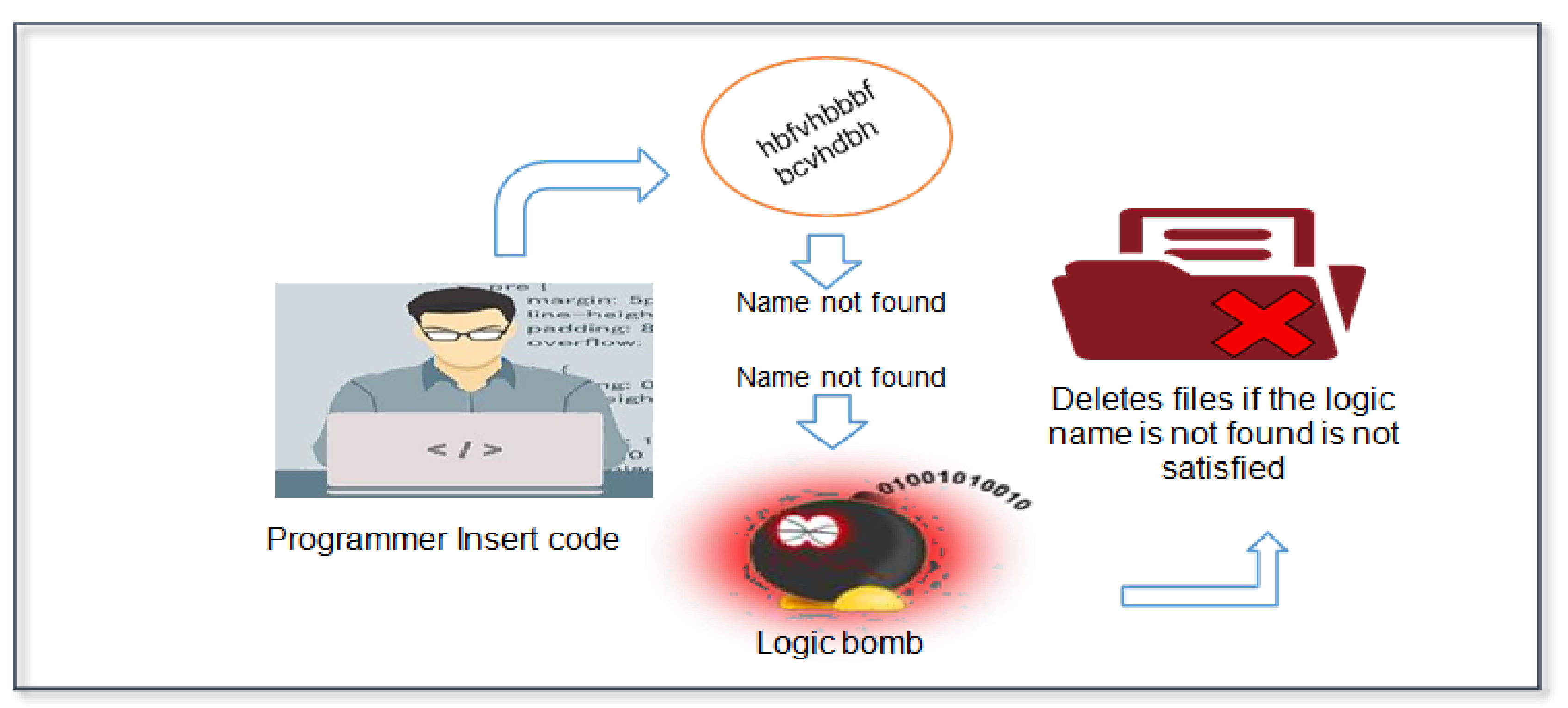


An example of Trojan Attack

- The figure describes that an attacker sends a Trojan virus to the victim’s system
- This infects the target victim’s system and the victim system’s IP address and port information passes through the ICQ server and reaches the attacker system
- ICQ server is a cross-platform instant messaging and VoIP that monitors for possible attacks
- After that, the attacker establishes connection and directly takes over the victim’s system causing damages to the files and information present in it

- **Logic bombs**

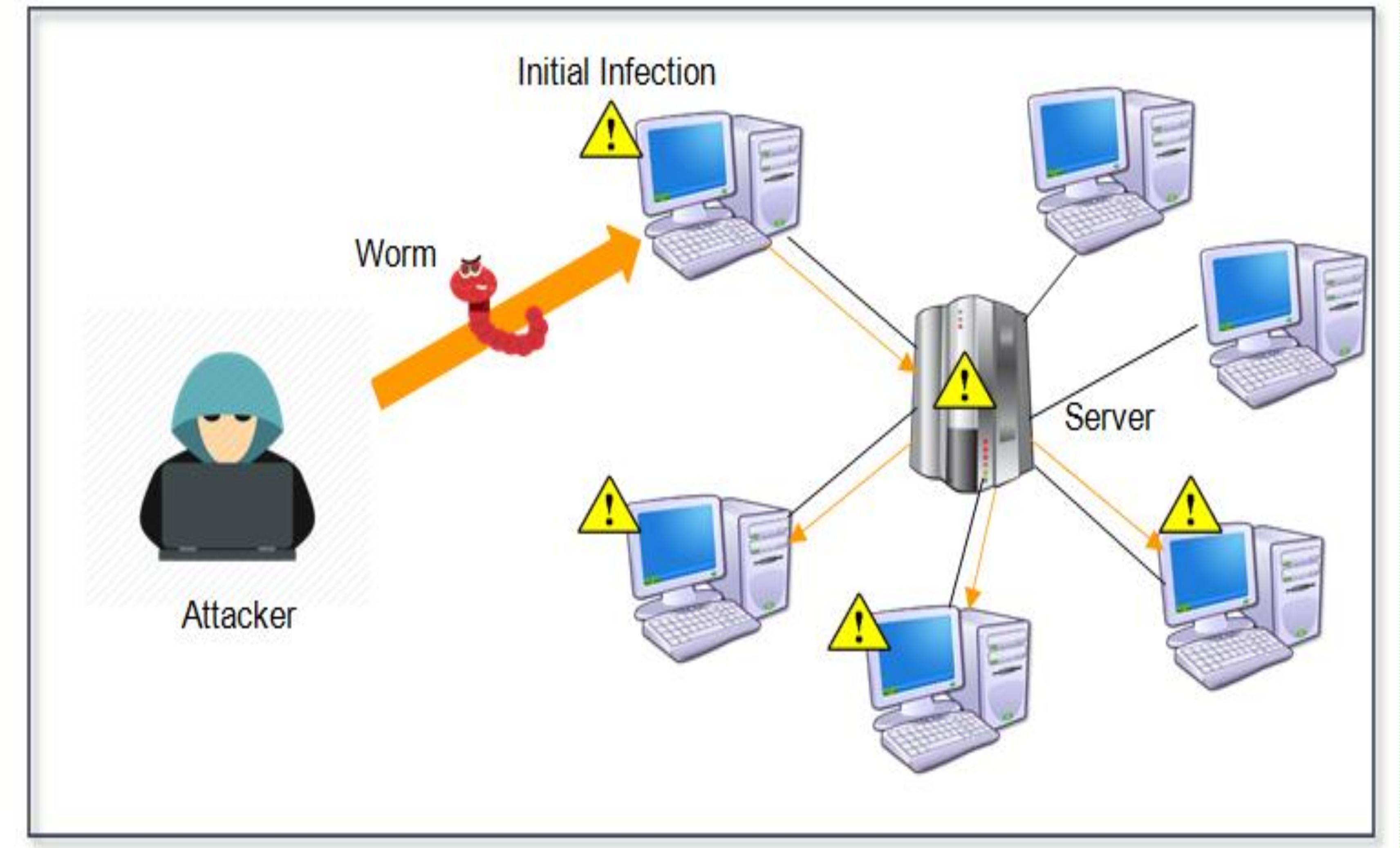
- Logic bombs are added with an application and get triggered when a specific scenario, like specific date and time or logical condition is satisfied



An example of Logic Bombs

- **Worms**

- Worms are self-contained programs that propagate across computers and networks
- It is different from viruses and is not attached with host file
- Typically, it is transferred via emails. While opening the attachments in the email the worms get activated.
- Worms send copy to each and every contact in the infected computer’s email addresses.
- It also conducts malicious activities like spreading across the Internet and overloads the server’s email which results in Denial-of-Service (DoS) attacks in the network



An example of Worm Attack

- **Droppers**

- Droppers are a program which is used to download and install viruses on a computer system
- Dropper is not infected with malicious code since it cannot be detected by virus scanning software. It automatically connects to the Internet and then downloads the updates for the virus software on a system

- **Ransomware**

- It demands for ransom to be paid. Till it is paid, it controls and blocks the victim’s information access and further looms to delete them.
- There are two types of ransomware namely **simple and advance**
- A simple computer ransomware locks the system in such a way that it is not possible even for a skilled person to unlock it
- Crypto viral extortion is a technique used by advanced ransomware.
- It encrypts the victim’s data in such a way that it is highly impossible for them to recover without the decryption key

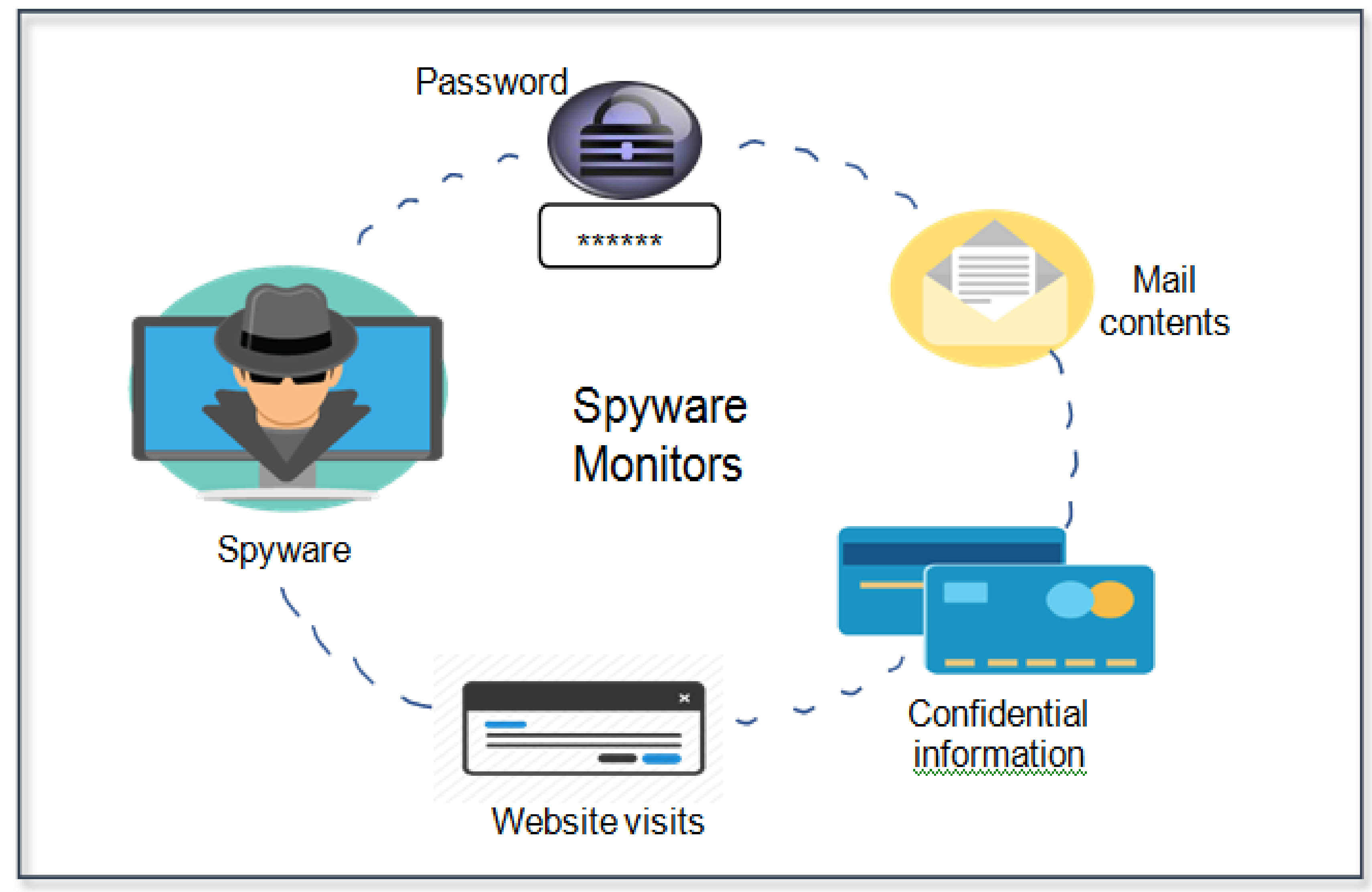
- **Adware**

- Adware is used by the companies for marketing and advertising banners
- They are displayed when any kind of program is running in the machine
- While browsing any kind of website, through a bar it appears on the computer screen automatically and can be viewed through pop-up and it can be downloaded to the system

An example of Adware

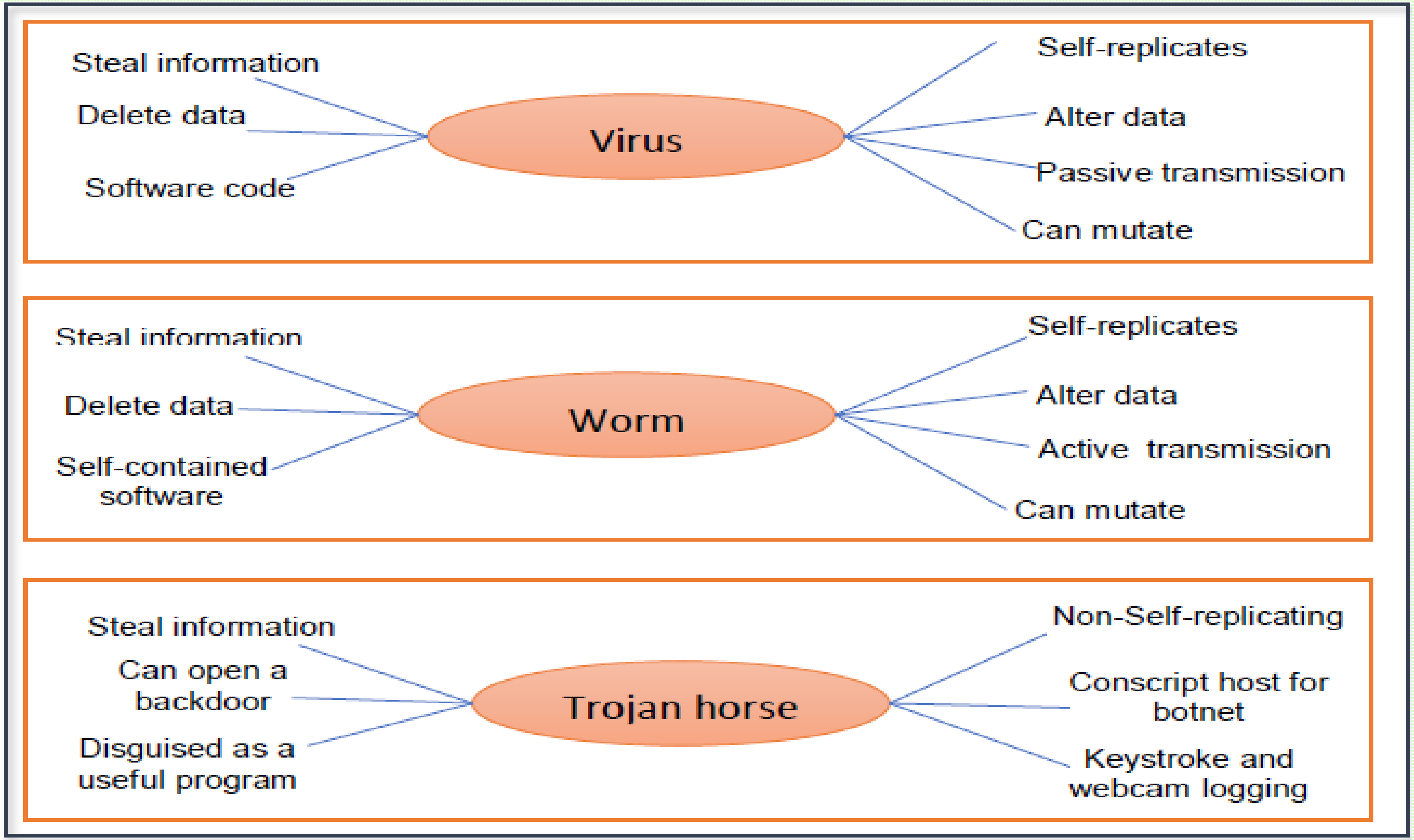
- **Spyware**

- It is a type of program that could be installed on the system to gather the useful information about the users and their computers along with their browsing habits
- Without the knowledge of the user, it tracks all the activities and forwards the report to the unknown remote user/hacker
- It also tries to install the malicious codes which are downloaded from the Internet
- It can installed in the machine when a freeware application is downloaded unknowingly with user
- It works exactly like an adware and it works like a separate program



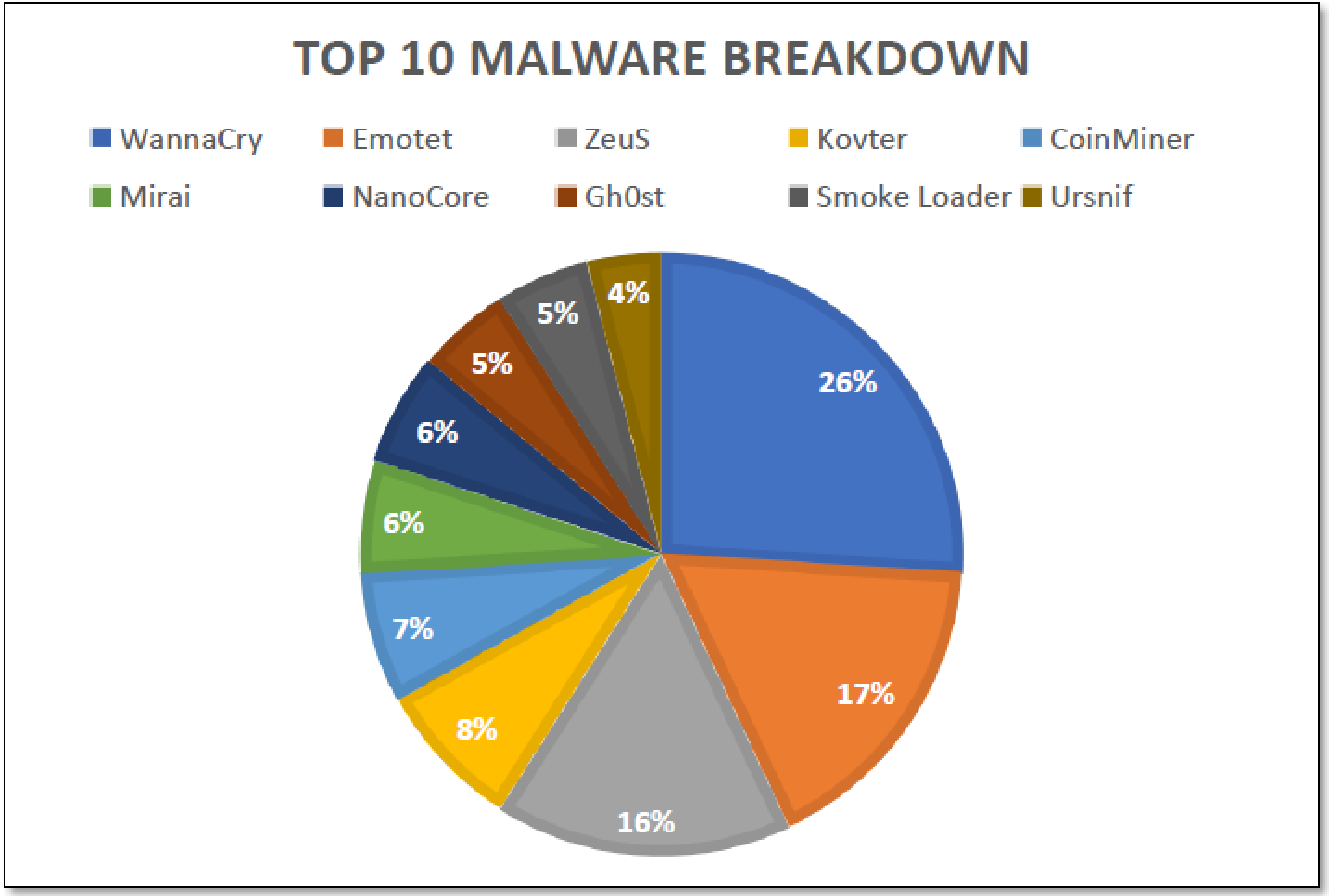
Spyware Example

Similarities and Differences between Virus, Worms and Trojan horse



TOP 10 MALWARE BREAKDOWN

- According to the statistics reported to Multi-State Information Sharing Analysis Centre (MS-ISAC) the latest top ten malware breakdown from on November 2018
- The statistics is collected based on the monitoring of different malware behavior and the effects due to the malwares reported to MS-ISAC from October 2018 to November 2018



Top 10 Malware Breakdown according to MS-ISAC report

- **Top 10 types of malware reported to MS - ISAC**
- WannaCry is a Ransomware malware
- Emotet is an integrated infostealer that downloads or drops Trojans.
- ZeuS is also an integrated banking Trojan.
- Kovter is a kind of adware that possess backdoor abilities.
- CoinMiner is also a type of ransomware.
- Mirai is a malware Botnet.
- NanoCore is a Remote Access Trojan (RAT).
- Gh0st is a RAT that is dropped by other malware and has backdoor abilities.
- Smoke Leader is distributed by malicious spams.
- Ursnif is a type of banking trojans.

COMMON CYBER ATTACK TERMS

- Based on these types of attacks, exploits and threats which are evolving various terms are also identified to describe them.
- Few of the most common terms are as follows:
  - **Hacker**
  - **Cracker**
  - **Phreaker**
  - **Spammer**
  - **Phisher**
  - **White hat**
  - **Black hat**

- **Hacker**

- A term Hacker is commonly used to represent a computer programming expert, but most recently the term is used to represent an adverse any which describes an individual who attempts to get unauthorized access with malicious intent to any resources

- **Cracker**

- An individual who tries to get the unauthorized access to the system or network resources with malicious intent is called Cracker

- **Phreaker**

- An individual who influence the phone network to execute a function that are not allowed is called Phreaker

- Aim is to break the phone network via a payphone to make long distance free calls

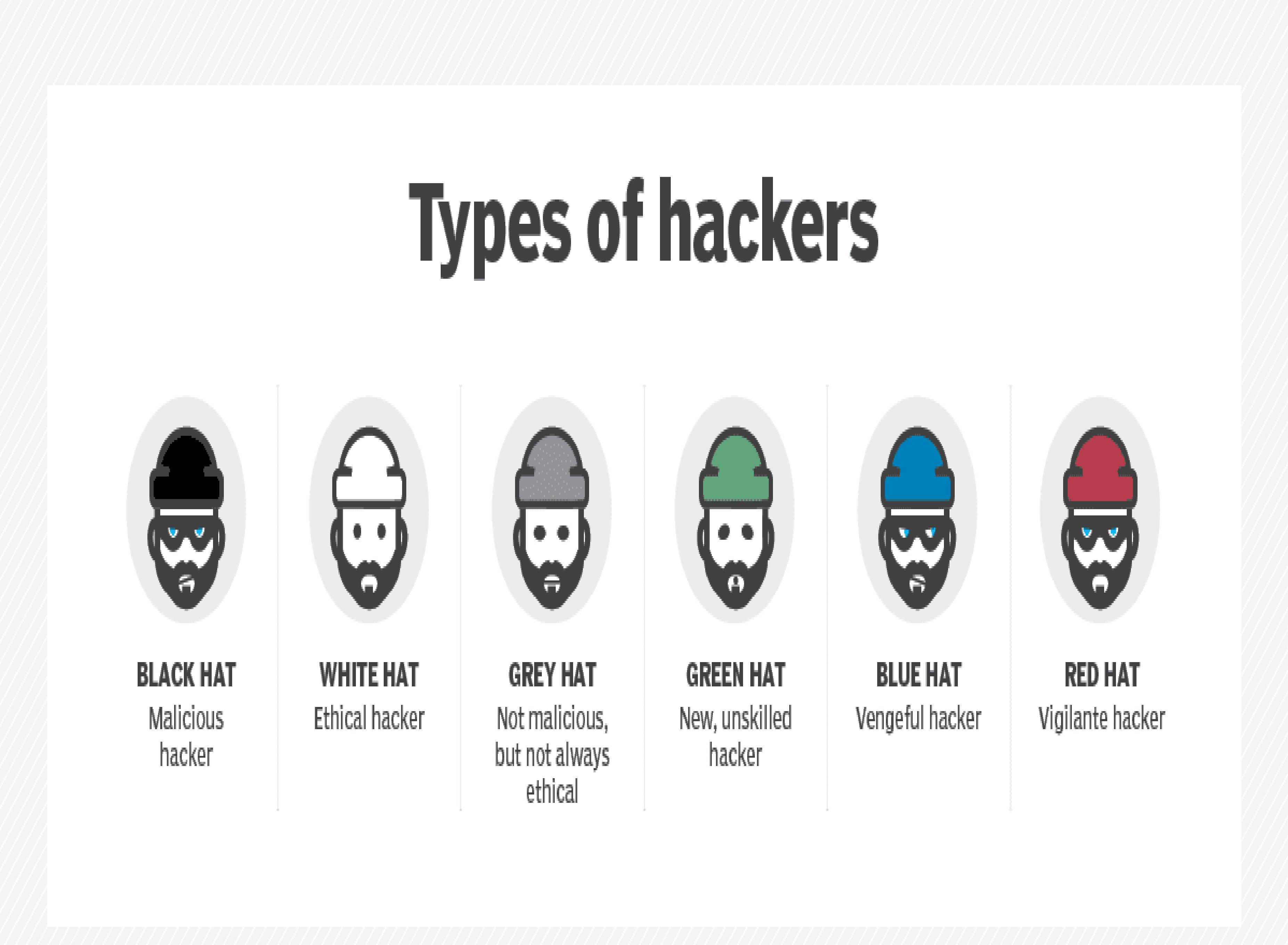
- **Spammer**

- An individual who sends huge number of unwanted emails is called spammer. They use viruses to take control of the system and sends out the bulk messages via mail

- **Phisher**

- The term Phisher is used to trick users to provide sensitive information like passwords, credit card numbers via email or by other means
- They pretend to be a trust worthy group and they have some genuine necessity for the sensitive information of the user

- **White hat**
- The term white hat is used to depict individuals they use their skill to find vulnerabilities in the networks
- These vulnerabilities are reported to the system owner who could fix it properly
- **Black hat**
- The term black hat refers to the individuals who use their computer skills to break into the network or systems that they don’t have authorized to access



Types of hackers

BLACK HAT
Malicious hacker

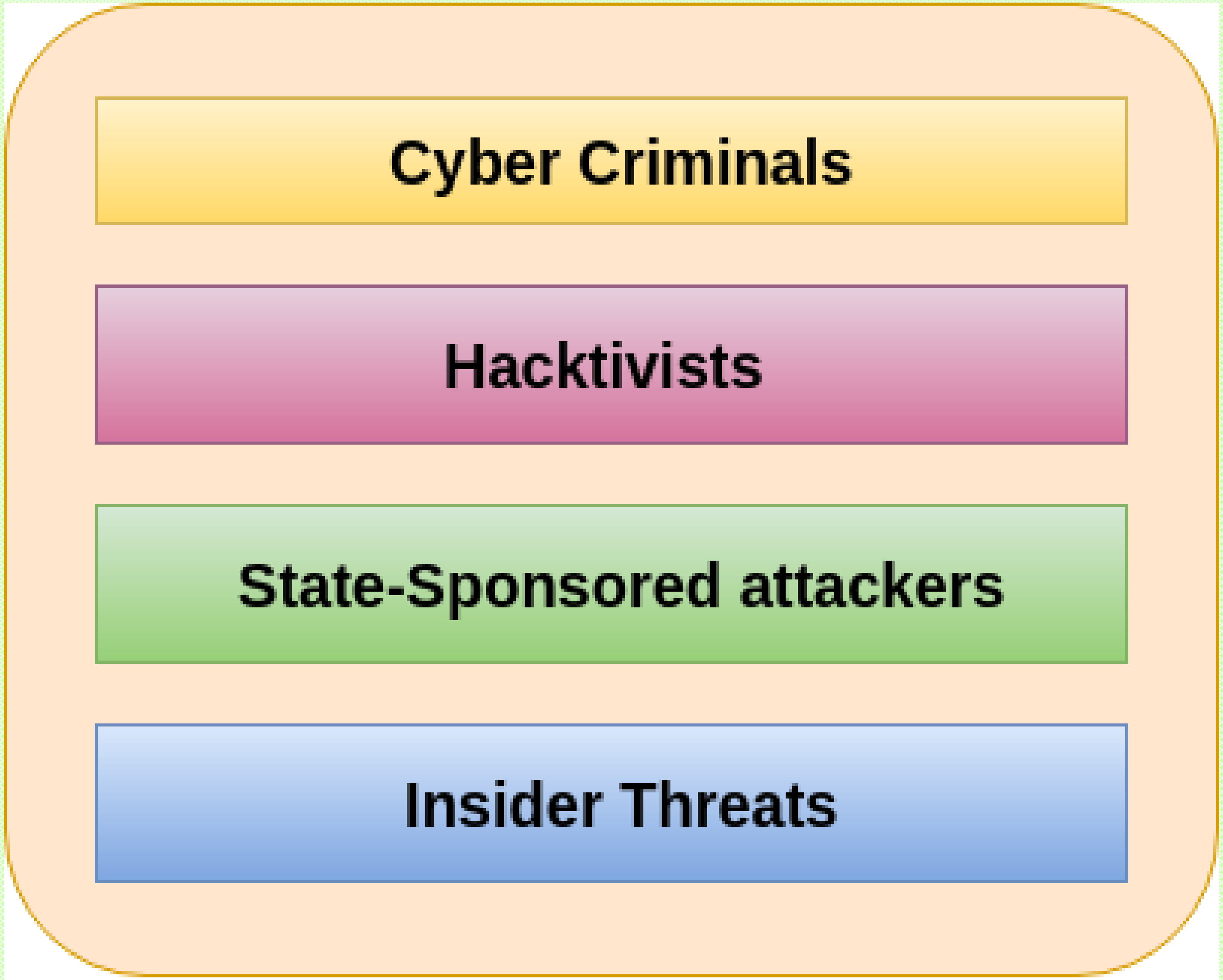
WHITE HAT
Ethical hacker

GREY HAT
Not malicious, but not always ethical

GREEN HAT
New, unskilled hacker

BLUE HAT
Vengeful hacker

RED HAT
Vigilante hacker



Cyber Criminals

Hacktivists

State-Sponsored attackers

Insider Threats

Types of CyberAttackers

- **Cyber Criminals**

- Cybercriminals are individual or group of people who use technology to commit cybercrime with the intention of stealing sensitive company information or personal data and generating profits. In today's, they are the most prominent and most active type of attacker
- **Cybercriminals use computers in three broad ways to do cybercrimes-**
- **Select computer as their target**- In this, they attack other people's computers to do cybercrime, such as spreading viruses, data theft, identity theft, etc
- **Uses the computer as their weapon**- In this, they use the computer to do conventional crime such as spam, fraud, illegal gambling, etc
- **Uses the computer as their accessory**- In this, they use the computer to steal data illegally

- **Hacktivists**

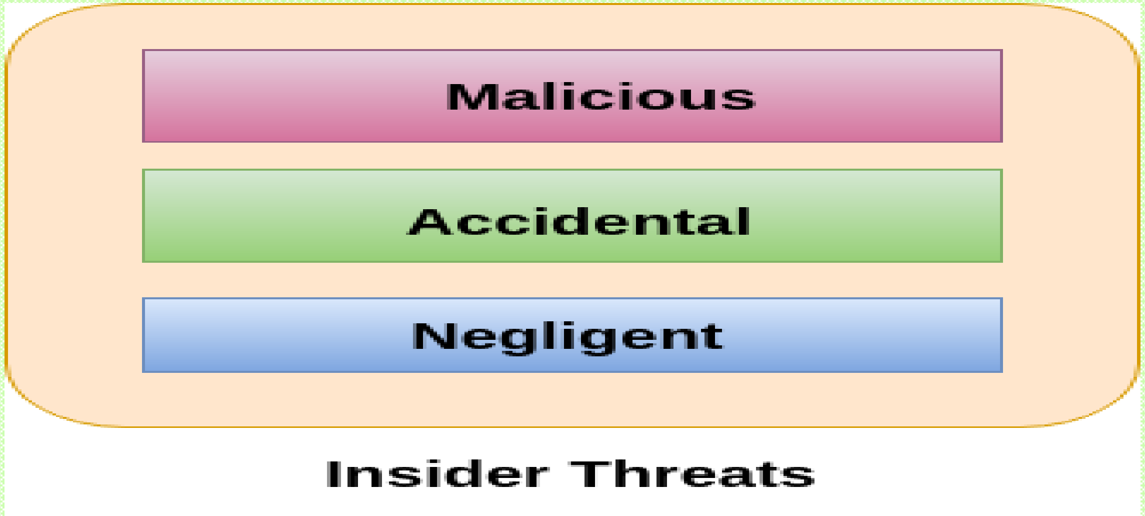
- Hacktivists are individuals or groups of hackers who carry out malicious activity to promote a political agenda, religious belief, or social ideology
- According to Dan Lohrmann, chief security officer for Security Mentor, a national security training firm that works with states said
- "Hacktivism is a digital disobedience. It's hacking for a cause"
- Hacktivists are not like cybercriminals who hack computer networks to steal data for the cash
- They are individuals or groups of hackers who work together and see themselves as fighting injustice

- **State-sponsored Attacker**

- State-sponsored attackers have particular objectives aligned with either the political, commercial or military interests of their country of origin
- The government organizations have highly skilled hackers and specialize in detecting vulnerabilities and exploiting these before the holes are patched
- It is very challenging to defeat these attackers due to the vast resources at their disposal

- **Insider Threats**

- The insider threat is a threat to an organization's security or data that comes from within
- These type of threats are usually occurred from employees or former employees, but may also arise from third parties, including contractors, temporary workers, employees or customers
- Insider threats can be categorized below-



- **Malicious**

- Malicious threats are attempts by an insider to access and potentially harm an organization's data, systems or IT infrastructure
- These insider threats are often attributed to dissatisfied employees or ex-employees who believe that the organization was doing something wrong with them in some way, and they feel justified in seeking revenge
- Insiders may also become threats when they are disguised by malicious outsiders, either through financial incentives or extortion

- **Accidental**

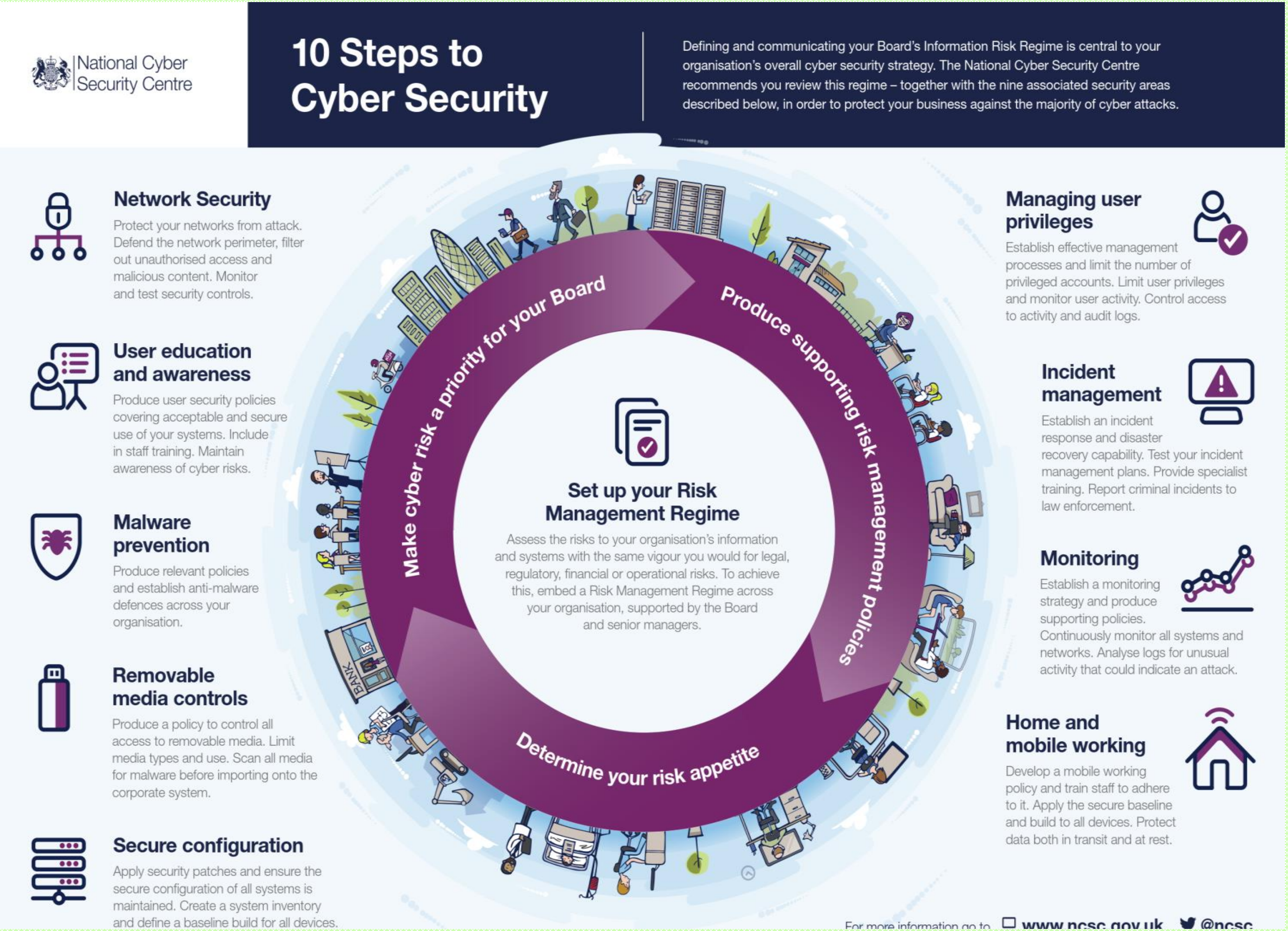
- Accidental threats are threats which are accidently done by insider employees. In this type of threats, an employee might accidentally delete an important file or inadvertently share confidential data with a business partner going beyond company? policy or legal requirements.

- **Negligent**

- These are the threats in which employees try to avoid the policies of an organization put in place to protect endpoints and valuable data. For example, if the organization have strict policies for external file sharing, employees might try to share work on public cloud applications so that they can work at home. There is nothing wrong with these acts, but they can open up to dangerous threats nonetheless.

SUMMARY

- The topic on classification of cyber attacks provides an overview on the different categories of Cyber-attacks involved in computer networks.
- The major topics covered are: The History of Cyber-attack, definition of cyber-attack, its characteristics and the attack types.
- The purpose and motivation of cyber-attack are described which provides a basic understanding of how and why it takes place.
- Cyber-attacks classification portrays various attack types based on purpose, severity of involvement, scope, legal classification and network types.
- Vulnerabilities and threats are major cause or consequence of a cyber-attack.
- Hence, those Vulnerability occurs due to several weakness in computer system, so one must have to protect their system by following system protection measures using antivirus software's and firewalls etc…



National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Make cyber risk a priority for your Board

Produce supporting risk management policies

Determine your risk appetite

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

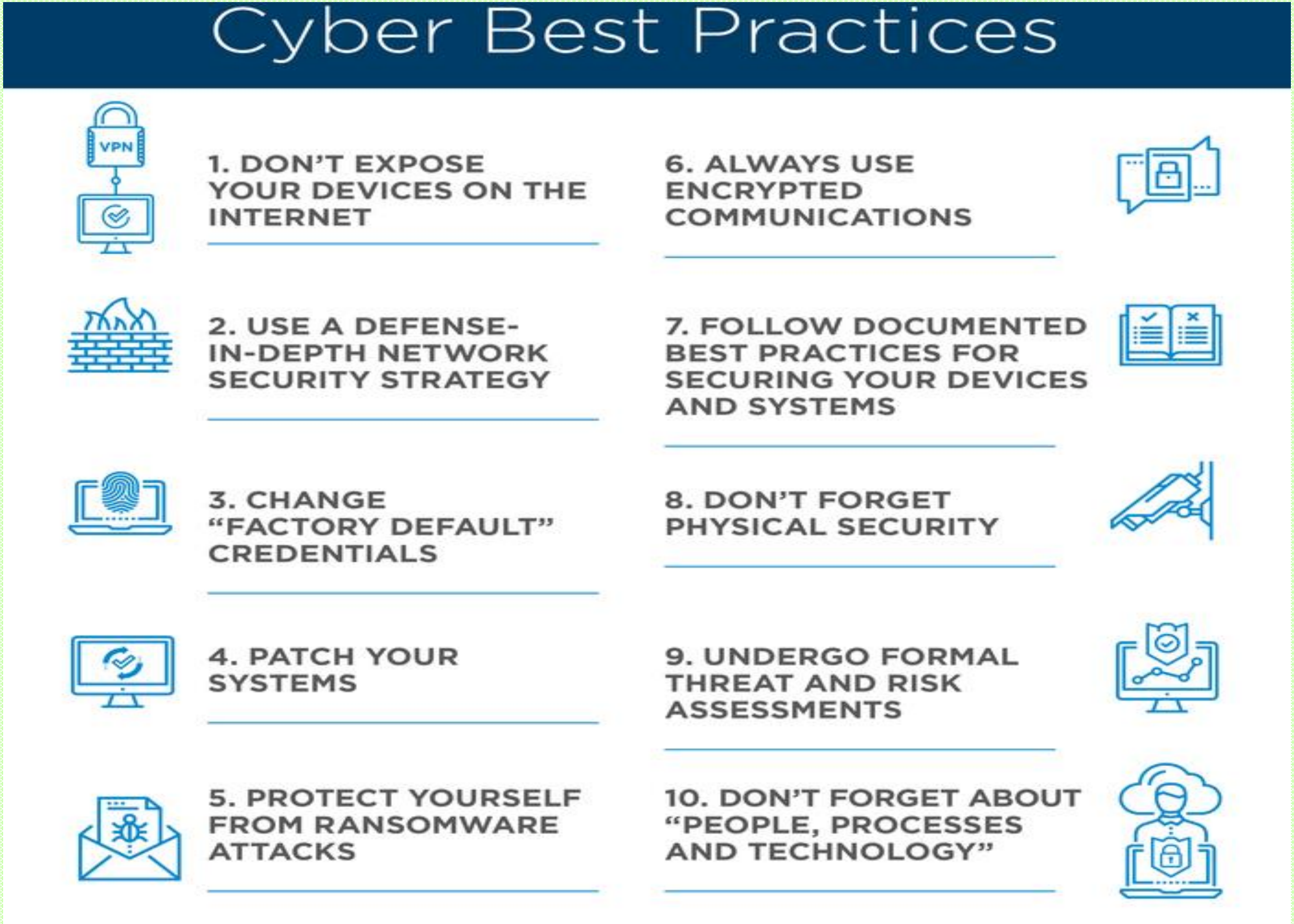
Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc



Cyber Best Practices

1. DON'T EXPOSE YOUR DEVICES ON THE INTERNET

2. USE A DEFENSE-IN-DEPTH NETWORK SECURITY STRATEGY

3. CHANGE "FACTORY DEFAULT" CREDENTIALS

4. PATCH YOUR SYSTEMS

5. PROTECT YOURSELF FROM RANSOMWARE ATTACKS

6. ALWAYS USE ENCRYPTED COMMUNICATIONS

7. FOLLOW DOCUMENTED BEST PRACTICES FOR SECURING YOUR DEVICES AND SYSTEMS

8. DON'T FORGET PHYSICAL SECURITY

9. UNDERGO FORMAL THREAT AND RISK ASSESSMENTS

10. DON'T FORGET ABOUT "PEOPLE, PROCESSES AND TECHNOLOGY"

THANK YOU...