Introducing myself

Dr. Zakria

PhD, Software Engineering

University of Electronic Science and Technology of China.

MS, Computer Science and Information Technology

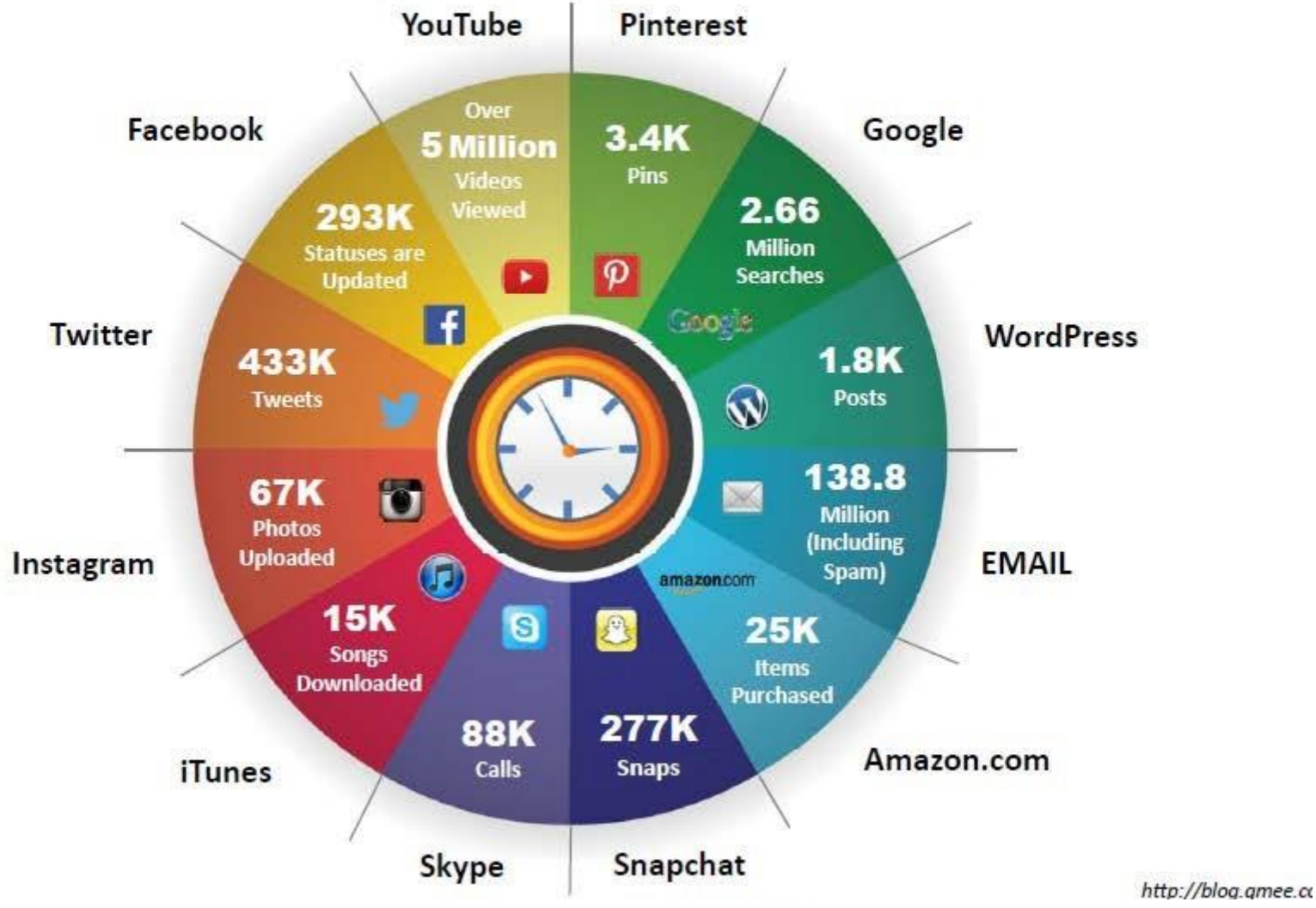
NED University of Engineering and Technology, Karachi.

BS, Computer Engineering

COMSATS University, Lahore, Pakistan

Internet is Integral part of business and personal life

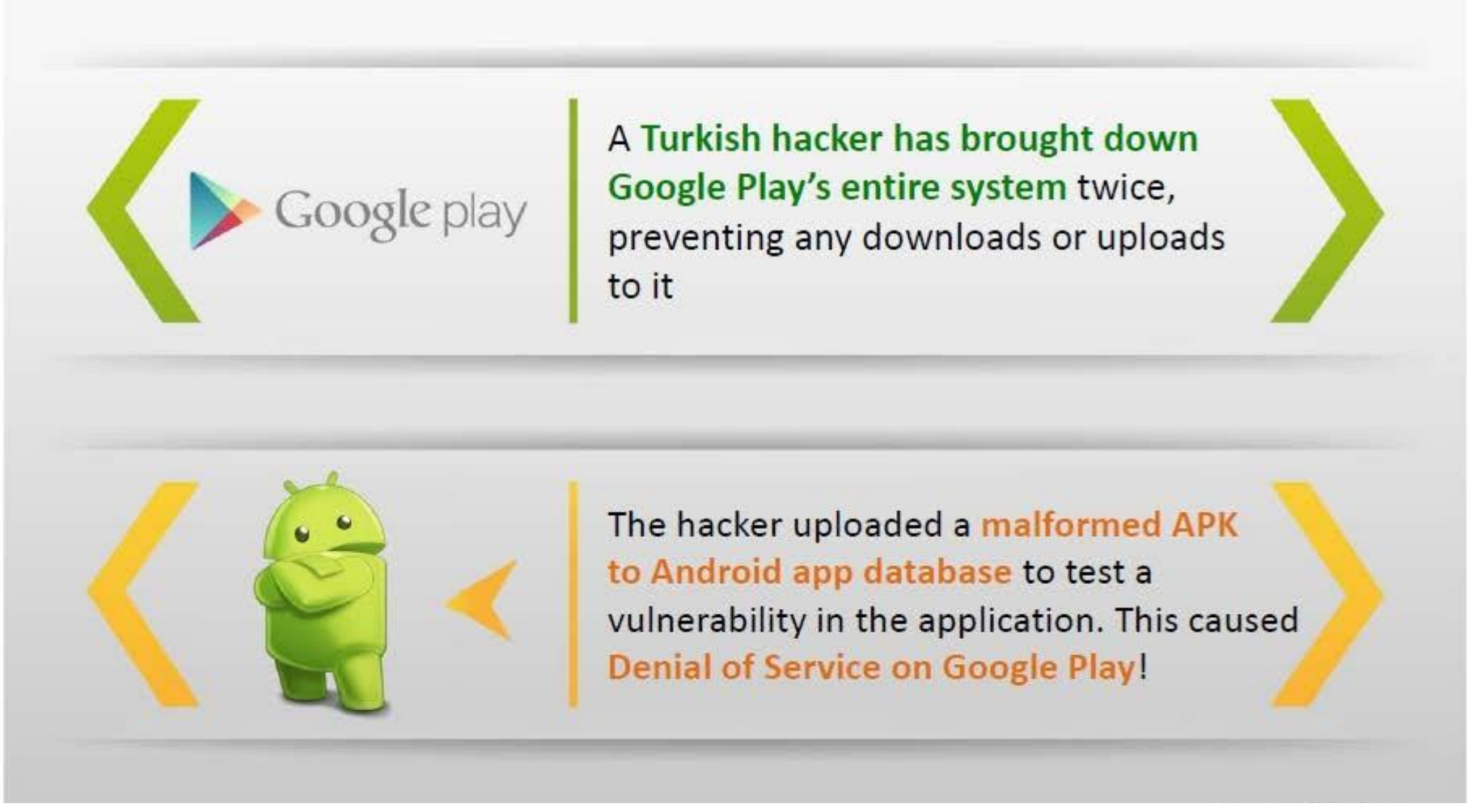
What happens online in 60 seconds



http://blog.qmee.cc

Case Study : Ebay data breach

Case Study : Google Play Hack



Case Study : The Home Depot data breach

Case Study : JP Morgan Chase data breach

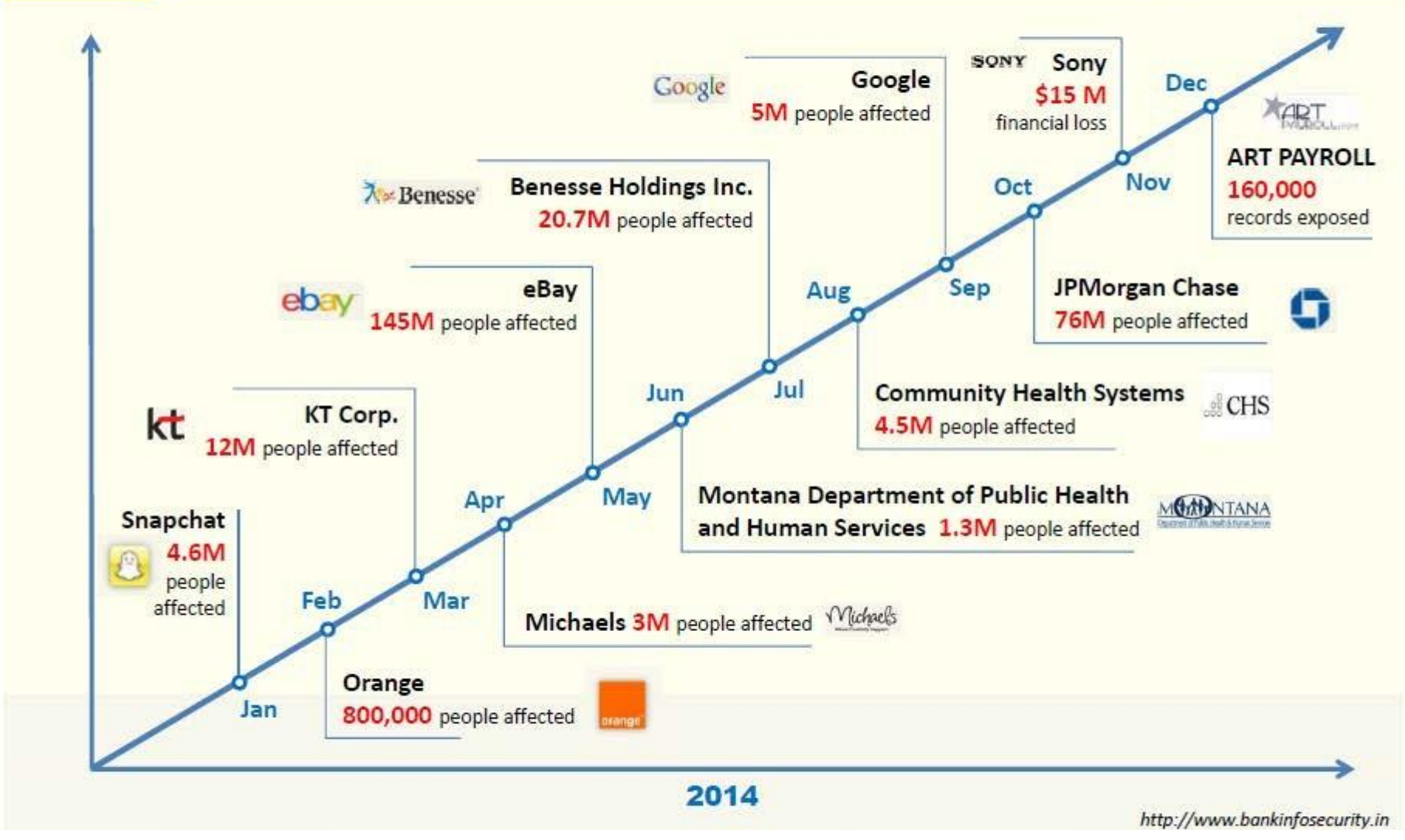
Contact information for **76 million households** and **7 million small businesses** were compromised

Incident occurred due to **attack on web applications**

JPMorganChase

http://dealbook.nytimes.com

Case Study : Year of Mega Breaches



Data Breach Statistics

There were over **3,007,682,404** data records lost or stolen since 2013 till Mar-2015

3,221,670 records lost **every day** in Jan-15

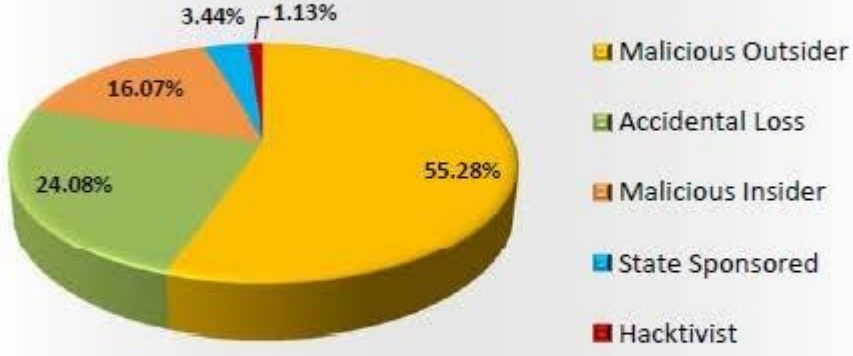
134,236 records **every hour**

2,237 records **every minute**

37 records **every second**

Data Records Lost/Stolen by Industry

Breach by Source



Source: http://breachlevelindex.com (Jan 2014 – Dec 2014)

What Is Security?

“A state of being secure and free from danger or harm; the actions taken to make someone or something secure.”

Security is not a ‘thing’ – rather, it is a ‘process.’

--

Cyber Security?

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.

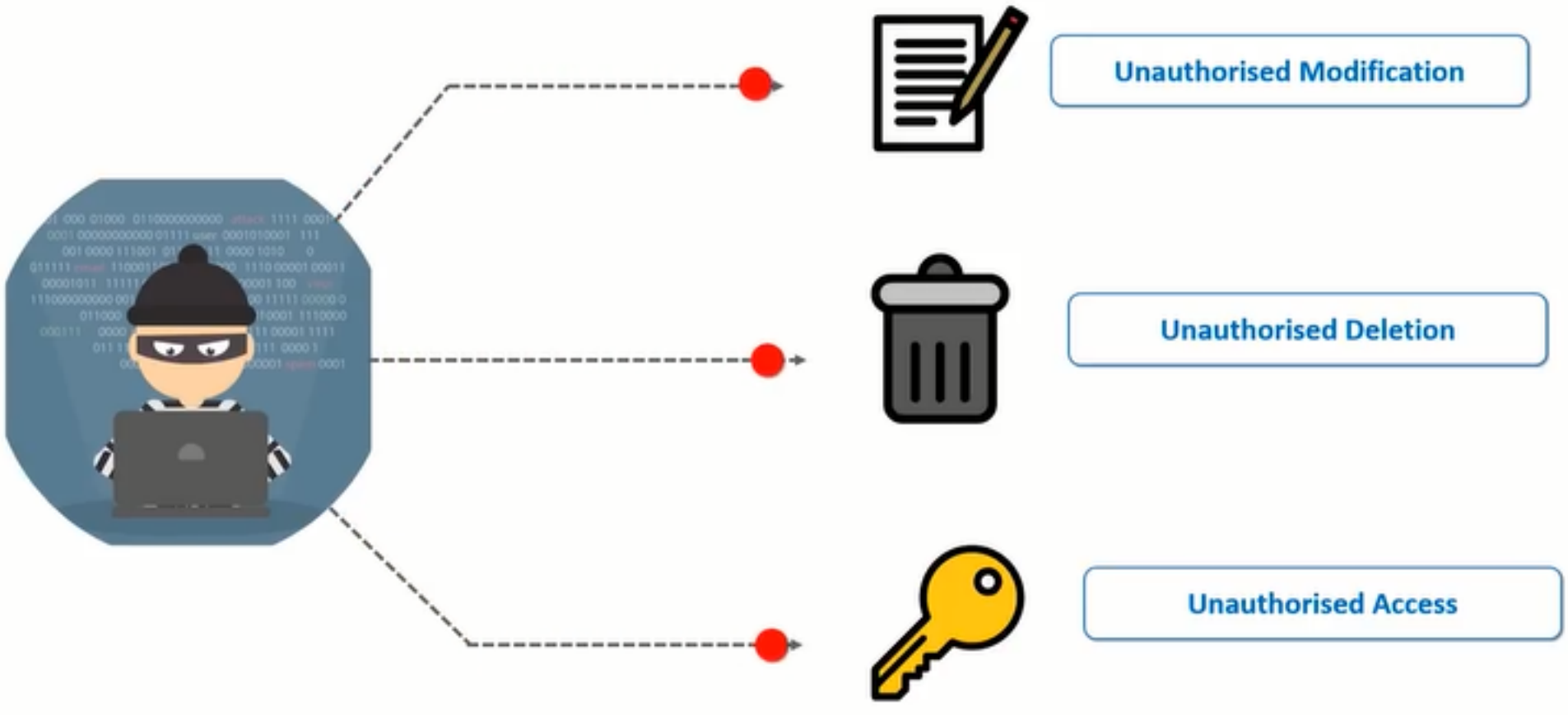
Cyber security?

Cyber security is the protection of Internet connected system, including hardware, software, and program or data from cyber attacks.

Precautions taken to guard against unauthorized access to data (in electronic form) or information systems connected with internet

Prevent crime related to Internet

Protect Against What?



C.I.A. triangle or Security Objectives

Confidentiality

> "Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information."

Integrity

> "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."

Availability

> "Ensuring timely and reliable access and use of information."

Attacks on CIA

Confidentiality

- Cracking Encrypted Data
- Man In The Middle attacks on plain text
- Data leakage/ Unauthorised copying of sensitive data
- Installing Spyware/Malware on a server

Integrity

- Web Penetration for malware insertion
- Maliciously accessing servers and forging records
- Unauthorised Database scans
- Remotely controlling zombie systems

Availability

- DOS/DDoS attacks
- Ransomware attacks – Forced encryption of Key data
- Deliberately disrupting a server rooms power supply
- Flooding a server with too many requests

Types of Attacks

Malware


MALWARE
Computer Virus
Worms
Spyware
Trojan Horse
Adware
110110
010101

Malware attack

Downloaded

Spyware

The most rapidly growing types of malware

- Cookies
- Key logger

Computer Worms

1. Can self-replicate

2. They do not need to attach themselves with existing programs

Computer Viruses

1. Can self-replicate

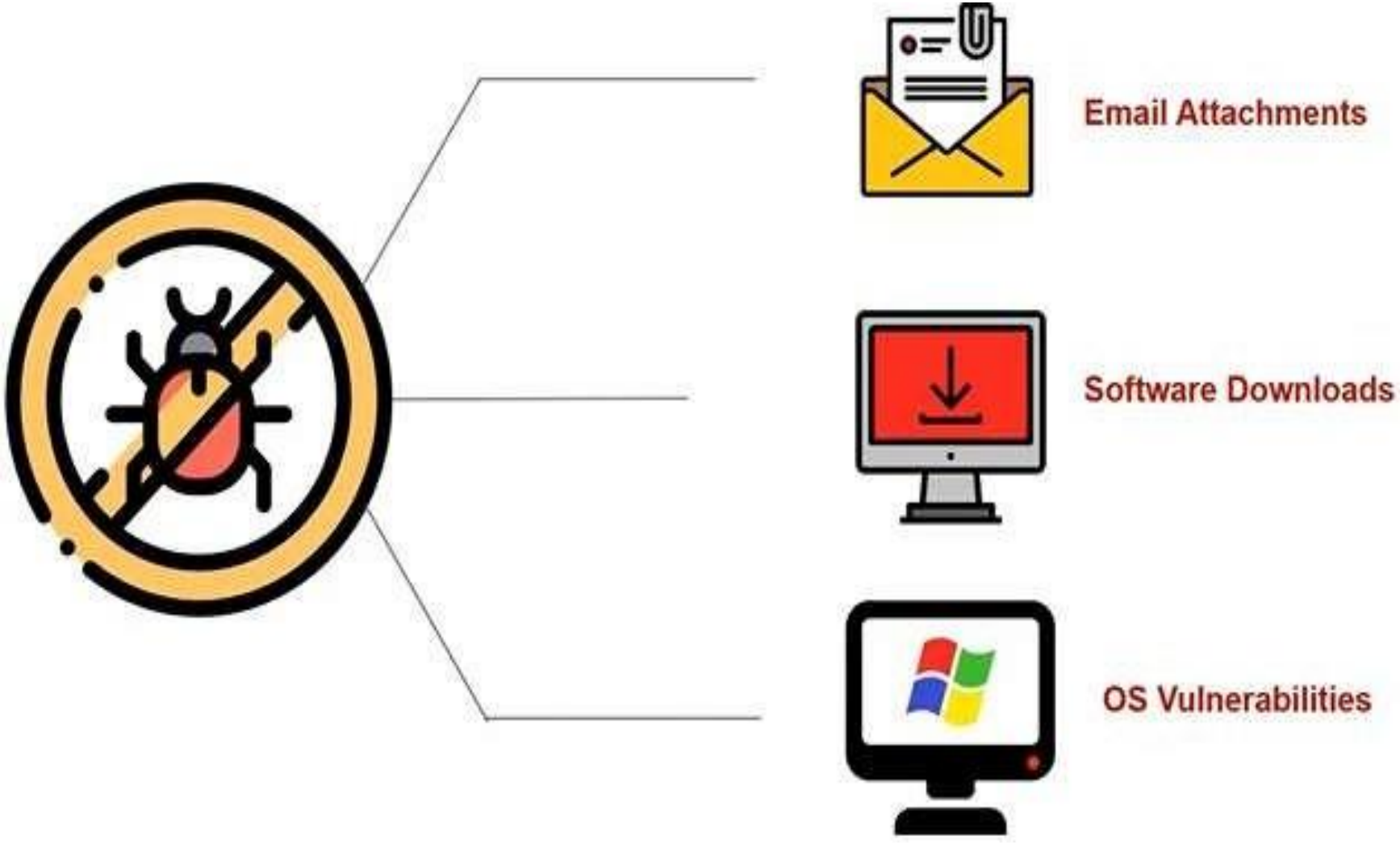
2. Attach themselves with existing programs

Trojan Horses

1. Cannot self-replicate

2. Use social engineering techniques to spread.

How Malware


Email Attachments
Software Downloads
OS Vulnerabilities

How to Stop?

Suspicious Links

- Stop clicking suspicious links
- Always study the URL consciously and make sure you are not on a counterfeit site

Updated Firewall

- Updating your firewall constantly is a great idea
- Firewalls prevent the transfer of large data files over the network in a hope to weed out attachments that may contain malware.

Updated OS

- It's also important to make sure your computer's operating system (e.g. Windows, Mac OS X, Linux) uses the most up-to-date security updates
- Software programmers update programs frequently to address any holes or weak points.

Phishing Attack

Most of the attacks on financial institutions the past 3 years have NOT been through brute force attacks on firewall appliances, it has been through acquiring users' passwords, this technique is called "Phishing"

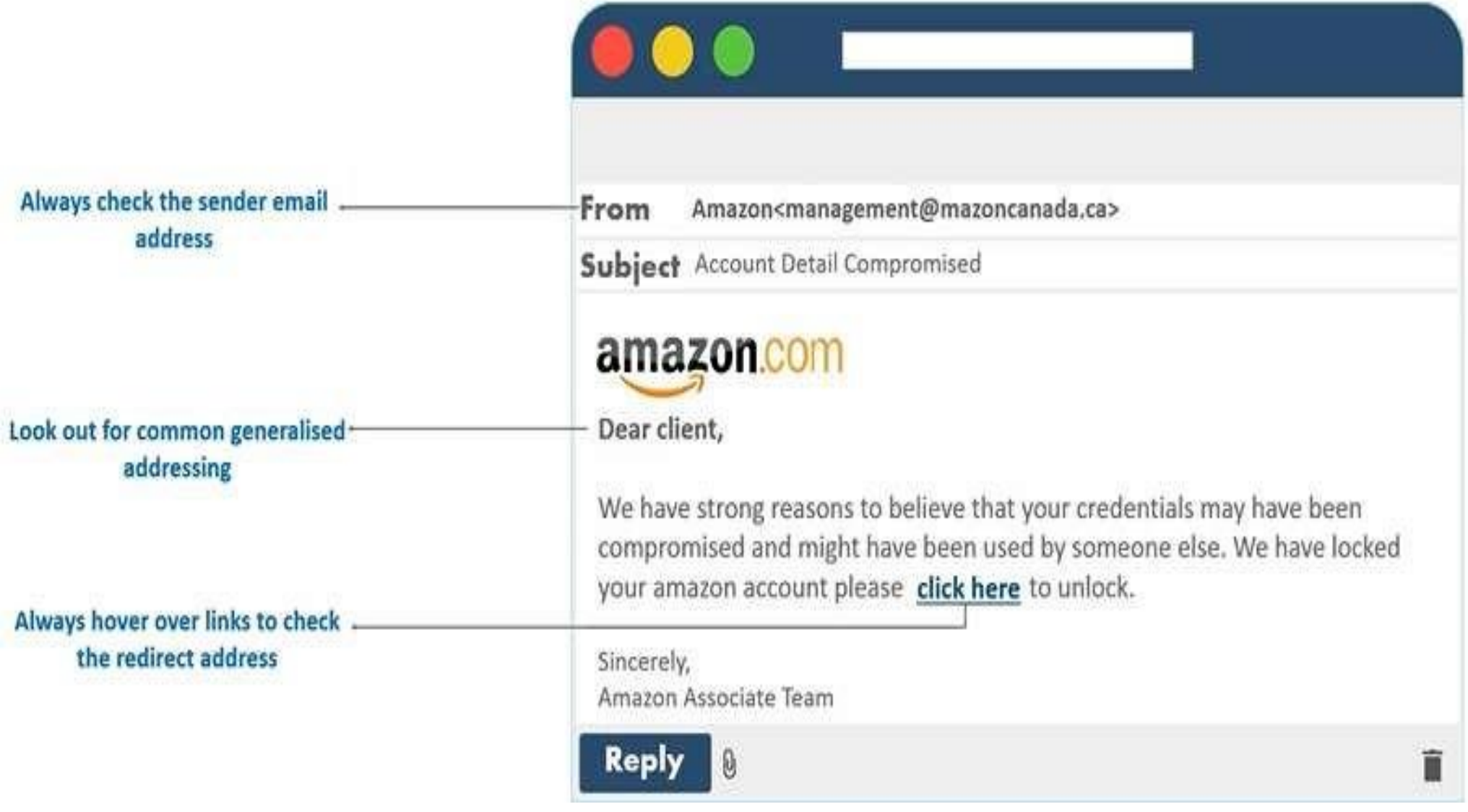
What is Phishing used for?

Stealing Confidential Data

Harvesting Login Credential

Impersonating

Phishing Awareness



Password Attacks

An attempt to obtain or decrypt a user's password for illegal use. Hackers can use cracking programs, dictionary attacks, and password sniffers in password attacks. Defence against password attacks is rather limited but usually consists of a password policy including a minimum length, unrecognizable words, and frequent changes.

Types of Password Attacks

Brute Force Attacks

Dictionary Attacks

Keylogger Attacks

Password Attack

1234, XYZ
ABCD, 3210

AABB, AATT
AACC, AAAC

Stop Password Attacks

Update Password

- It's always a great idea to keep changing essential passwords in regular intervals
- Passwords shouldn't be the same for everything

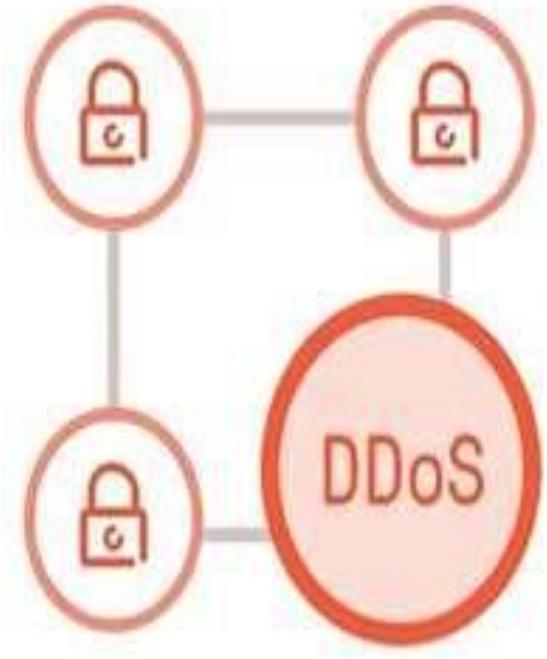
Use Alpha-Numeric

- When setting a password general best practices should be followed
- A password should contain a multitude of characters with a generous use of alpha numeric

NO Dictionary

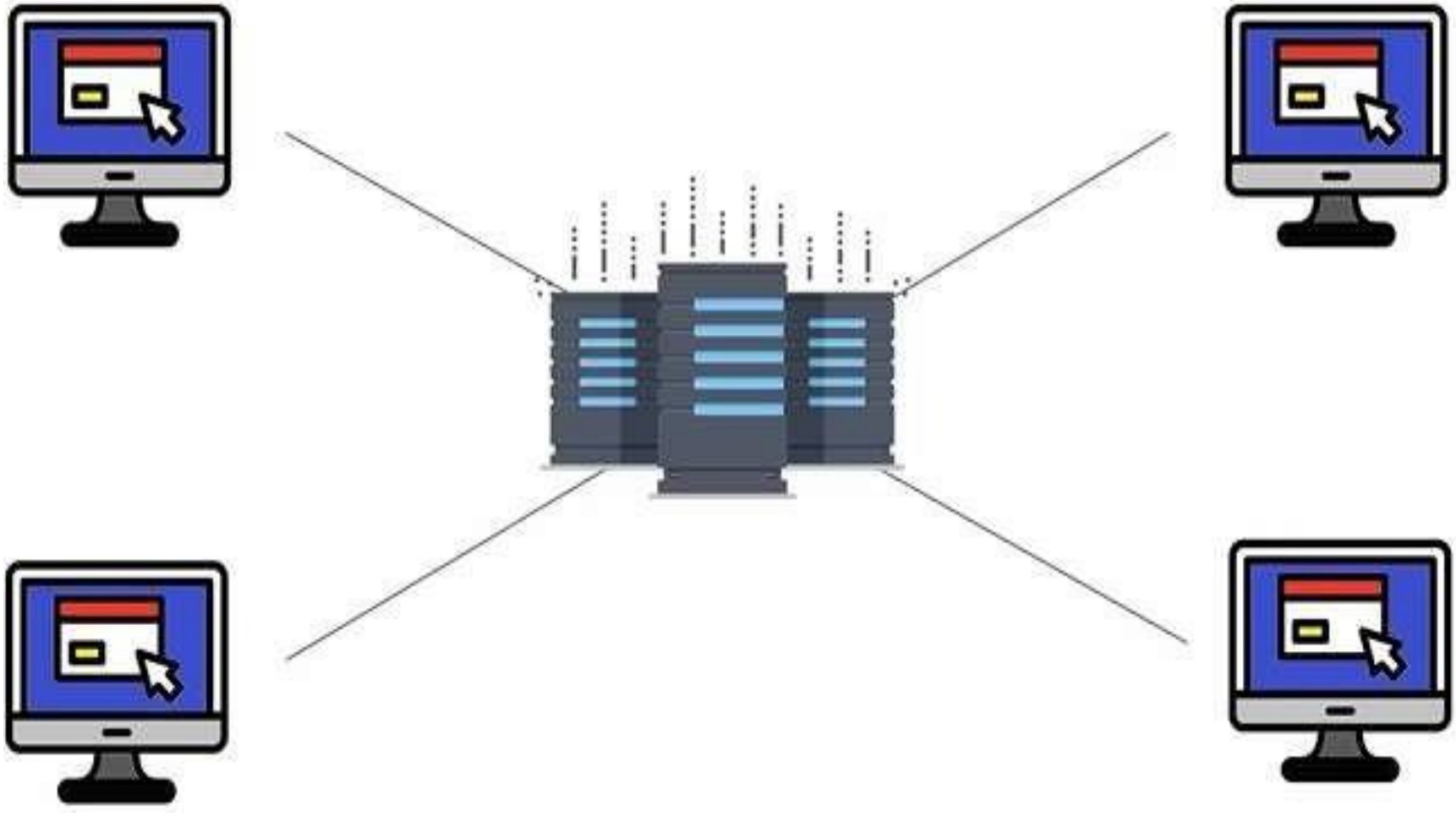
- It's always a great idea to use a password that only makes sense to you
- Passwords which use actual words that make sense are much more susceptible to dictionary attacks

Distributed Denial of Services (DDoS)



Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.

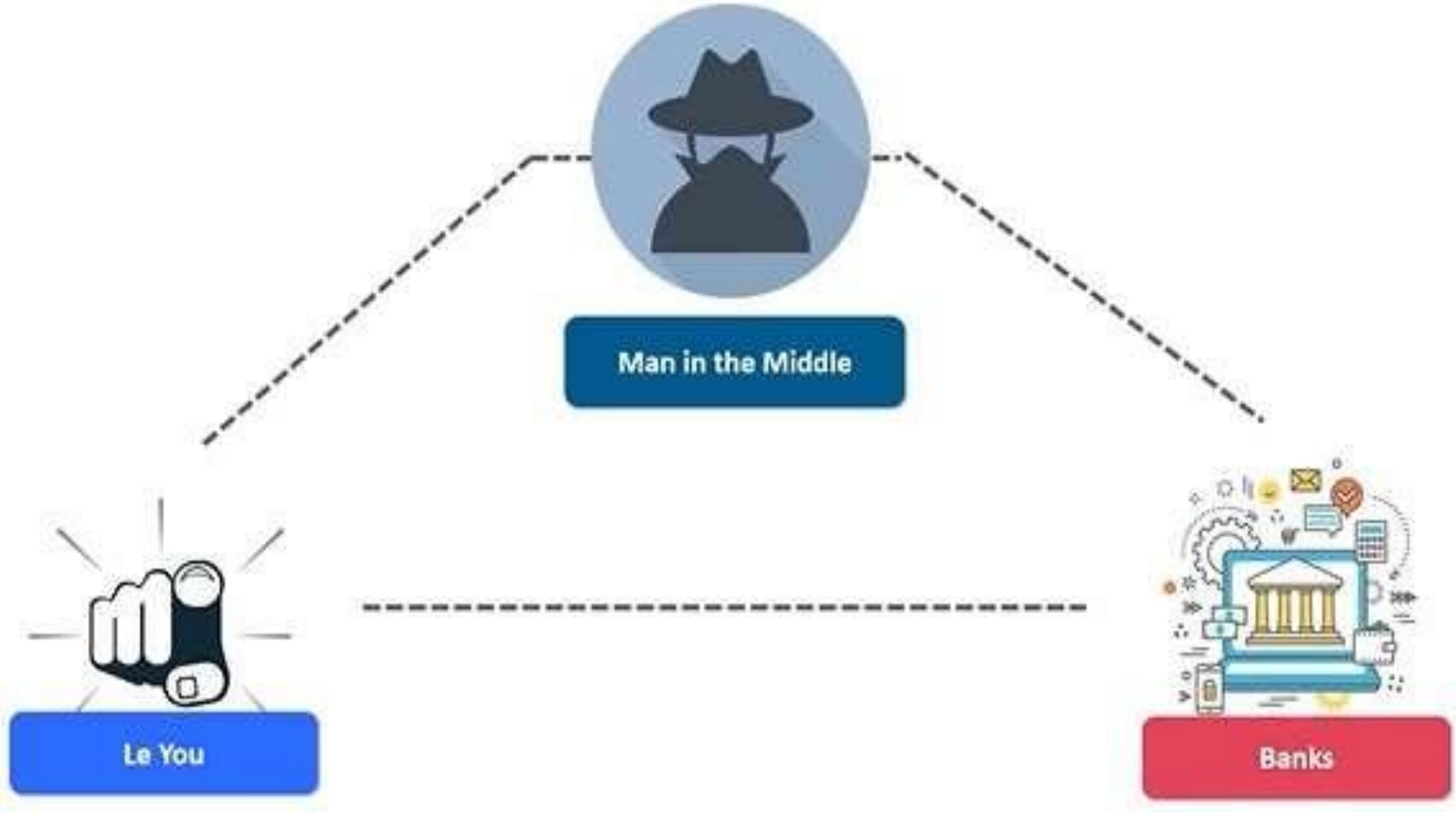
Packet Flood



Prevention

- Traffic Analysis
- Traffic Control
- Recovery Management

Man in the Middle



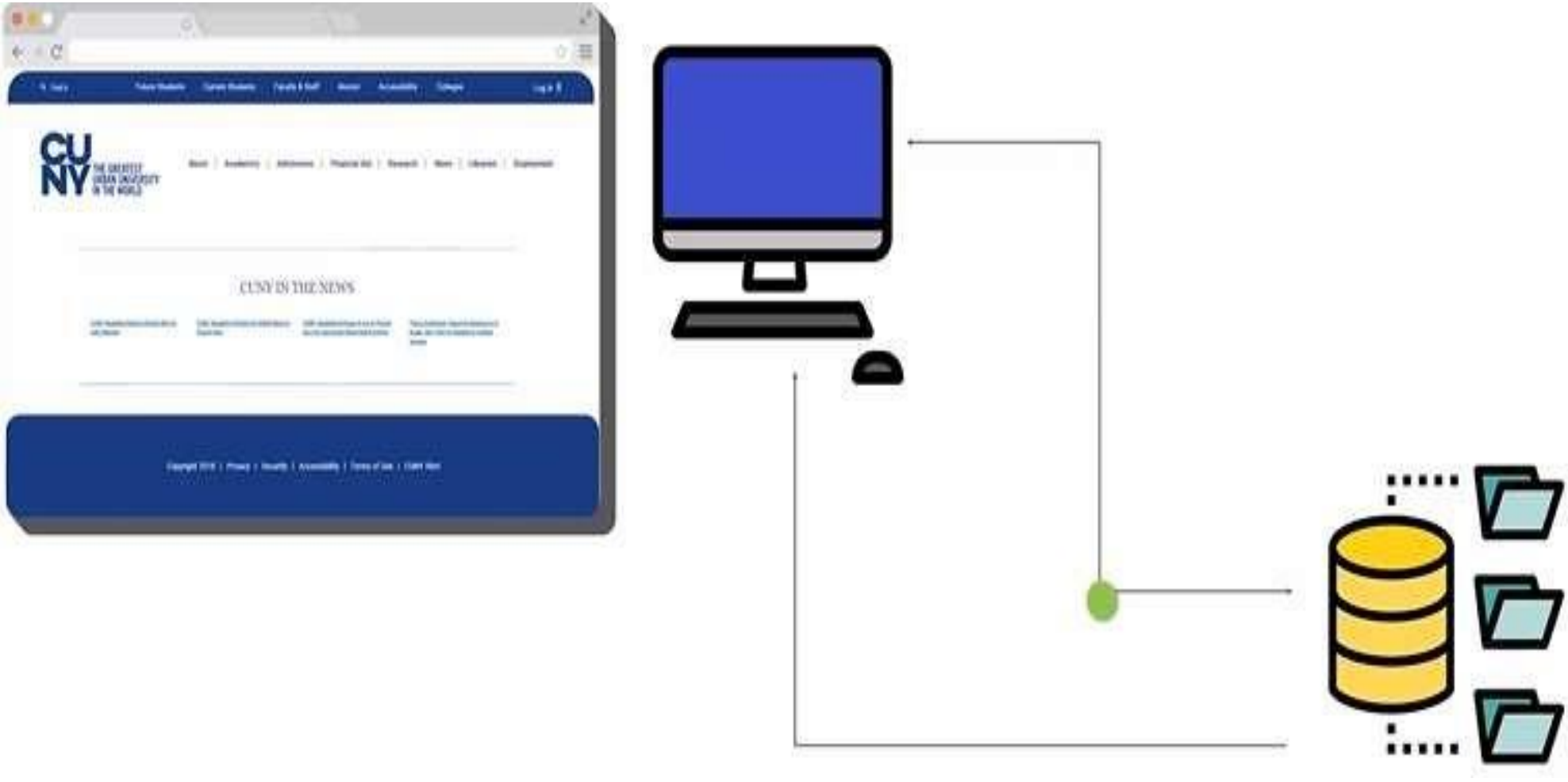
Prevent MITM

- Use encrypted WAP
- Always check the security of you connection(HSTS/HTTPS)
- Invest in a VPN

Drive-by Download

Drive-by download attacks occur when vulnerable computers get infected by just visiting a website. Findings from latest Microsoft Security Intelligence Report and many of its previous volumes reveal that Drive-by Exploits have become the top web security threat to worry about.

How it work?



Malvertising

Malvertising is the name we in the security industry give to criminally-controlled adverts which intentionally infect people and businesses. These can be any ad on any site – often ones which you use as part of your everyday Internet usage. It is a growing problem, as is evidenced by a recent US Senate report, and the establishment of bodies like Trust In Ads.

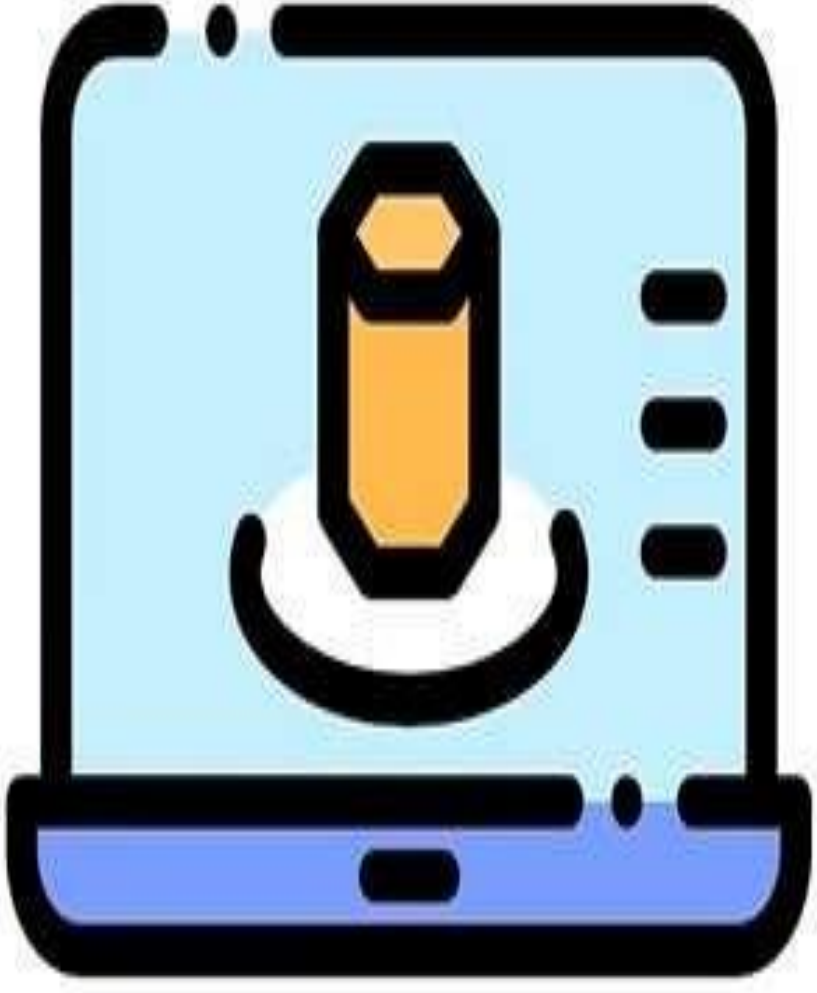
Prevention

Adblocker

Regular Software Updates

Common Sense

Rogue Software



Also called smitfraud, *scareware*, or *rogue security software*, this type of software is defined as malware - it is designed specifically to damage or disrupt a computer system. In this case, not only is the software going to disrupt your system, it's going to try and trick you into making a purchase using your credit card

Propagation

Prevention

Updated Firewall

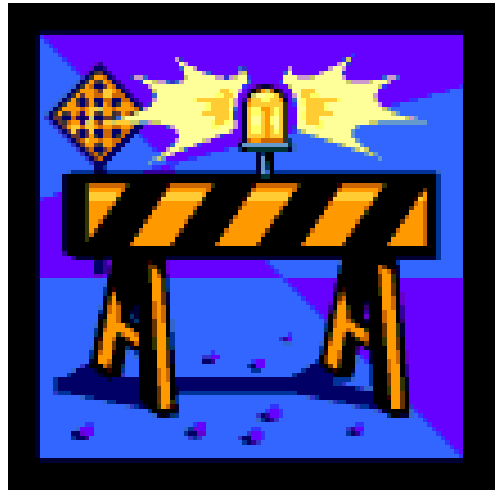
Use Efficient Antivirus

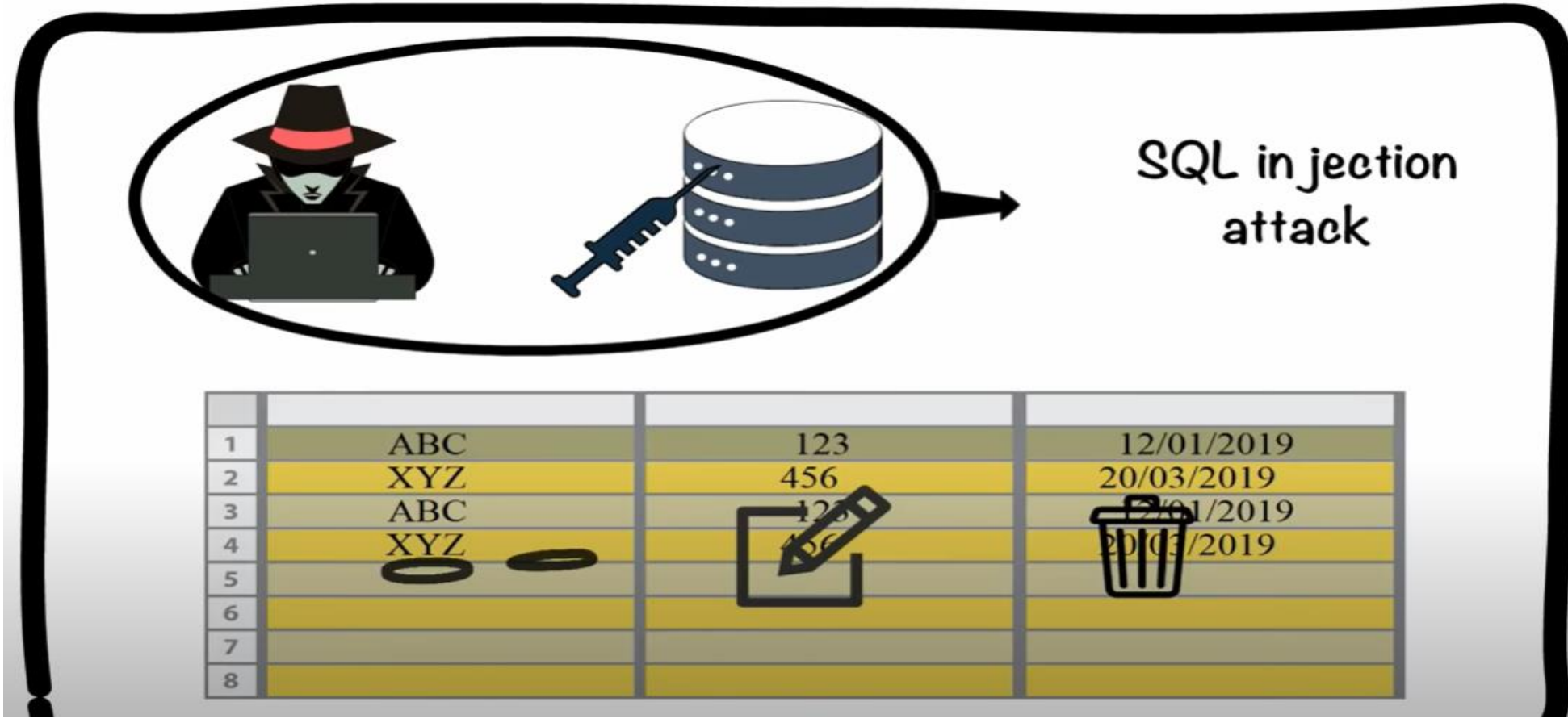
General Distrust

SQL injection

The attacker attempts to breach a web application. Common attacks of this type are SQL injection

This is a complex attack that involves actually taking over an authenticated session.




SQL injection attack
ABC 123 12/01/2019
XYZ 456 20/03/2019
ABC
XYZ

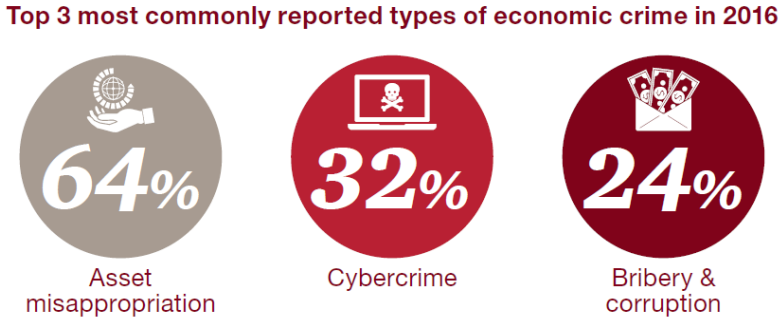
DNS Poisoning

This involves altering DNS records on a DNS server to redirect client traffic to malicious websites, usually for identity theft.

Cyber Crime?

Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. The computer may have been used source of a crime, or it may be the target.

IMPORTANCE OF INFORMATION SECURITY



As per PWC Global Economic Crime Report 2016, Cyber Crime was amongst the top 3 most commonly reported types of economic crime

As per Europol 2013 report, Cyber Crime is now more profitable than the drug trade

Classification of Cyber Crimes

- Insider Attack:
  - Person with authorized system access
  - Dissatisfied or unhappy inside employees or contractors
  - Motive could be revenge or greed
  - Well aware of the policies, processes, IT architecture and weakness of the security system
  - Comparatively easy for a insider attacker to steel sensitive information, crash the network, etc.
  - Could be prevented by using IDS/IPS

- External Attack:
  - Hired by an insider or an external entity to the organization
  - Organization not only faces financial loss but also the loss of reputation
  - Attackers usually scan and gathering information
  - Keeps regular eye on the log and carefully analyzing these firewall logs
  - IDS/IPS can also protect from external attackers

Classification of Cyber Crimes (Cont.)

- Cyber attacks can also be classified as:
  - Unstructured attacks
    - Generally person who don't have any predefined motives to perform the cyber attack
    - Try to test a tool readily available over the internet
  - Structure attacks:
    - Performed by highly skilled and experienced people
    - Motives of these attacks are clear in their mind
    - Access to sophisticated tools and technologies to gain access to other networks without being noticed
    - Expertise to develop or modify the existing tools to satisfy their purpose
    - Usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

Reasons for Commission of Cyber Crimes

- Money:
  - People are motivated towards committing cyber crime is to make quick and easy money.
- Revenge:
  - Take revenge with other person/organization/society/caste or religion
  - Defaming its reputation or bringing economical or physical loss.
  - This comes under the category of cyber terrorism.
- Fun:
  - The amateur do cyber crime for fun.
- Recognition:
  - It is considered to be pride if someone hack the highly secured networks
- Anonymity:
  - Anonymity that a cyber space motivates the person to commit cyber crime
- Cyber Espionage:
  - At times the government itself is involved in cyber trespassing to keep eye on other person/network/country

Kinds of Cyber Crimes

- Cyber Stalking
  - Stalking, harassing, threatening someone, or defame a person
  - The behavior includes false accusations, threats, sexual exploitation to minors, monitoring, etc.

  Child Pornography
  - Possessing image or video of a minor (under 18), engaged in sexual conduct.
- Forgery and Counterfeiting
  - Produce counterfeit which matches the original document
  - Not possible to judge the authenticity of the document
- Software Piracy and Crime related to IPRs:
  - An illegal reproduction and distribution
- Cyber Terrorism
  - Use of computer resources to intimidate or force government, the civilian population or any segment thereof in furtherance of political or social objectives
- Phishing
  - Acquiring personal and sensitive information of an individual via email
  - Vishing (voice phishing), Smishing

Kinds of Cyber Crimes (Cont.)

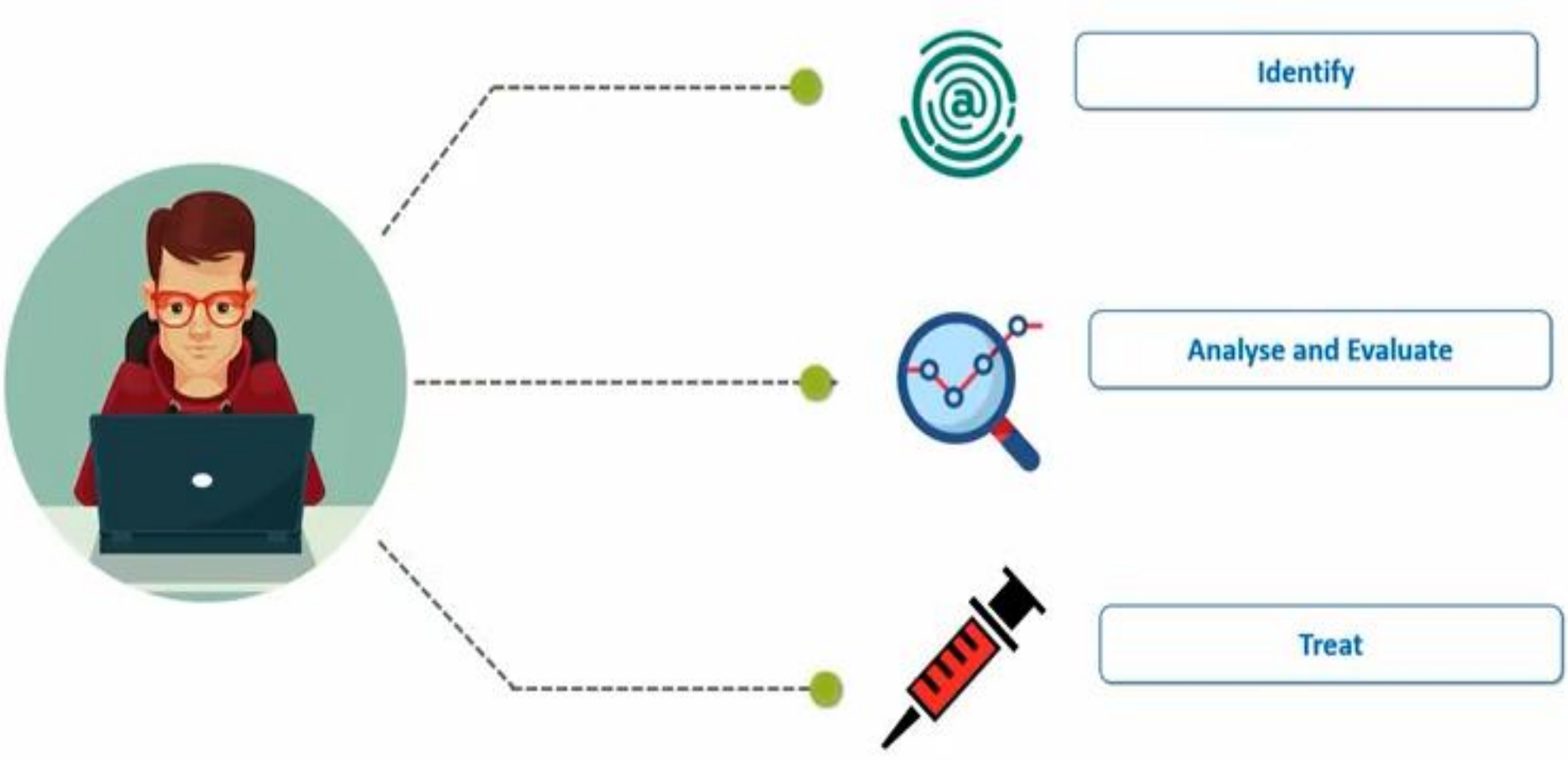
- Creating and distributing viruses over internet
  - Spreading of an virus can cause business and financial loss
- Spamming
  - Sending of unsolicited and commercial bulk message
  - Spams not only irritate the recipients and overload the network but also waste the time and occupy the valuable memory space

  Cross Site Scripting
  - Injecting a malicious client side script into a trusted website
  - Malicious script gets access to the cookies and other sensitive information and sent to remote servers
- Online Auction Fraud
  - Online auction fraud schemes which often lead to either overpayment of the product or the item is never delivered
- Cyber Squatting
  - Reserving the domain names of someone else's trademark
  - Sell it afterwards at higher price

Kinds of Cyber Crimes (Cont.)

- Computer Vandalism
  - Physical destroying computing resources using physical force or malicious code
- Computer Hacking
  - Modifying computer hardware and software to accomplish a goal
  - Simply demonstrations of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons

Steps to Fix a Crime



Essential Terminologies

Hack Value

It is the notion among hackers that **something is worth doing** or is interesting

Zero-Day Attack

An attack that exploits **computer application vulnerabilities** before the software developer releases a patch for the vulnerability

Vulnerability

Existence of a **weakness**, **design**, or **implementation error** that can lead to an unexpected event compromising the security of the system

Daisy Chaining

It involves **gaining access to one network and/or computer** and then using the same information to gain access to multiple networks and computers that contain desirable information

Exploit

A **breach** of IT system security through vulnerabilities

Doxing

Publishing personally identifiable information about an individual collected from publicly available databases and social media

Payload

Payload is the **part of an exploit code** that performs the intended malicious action, such as destroying, creating backdoors, and hijacking computer

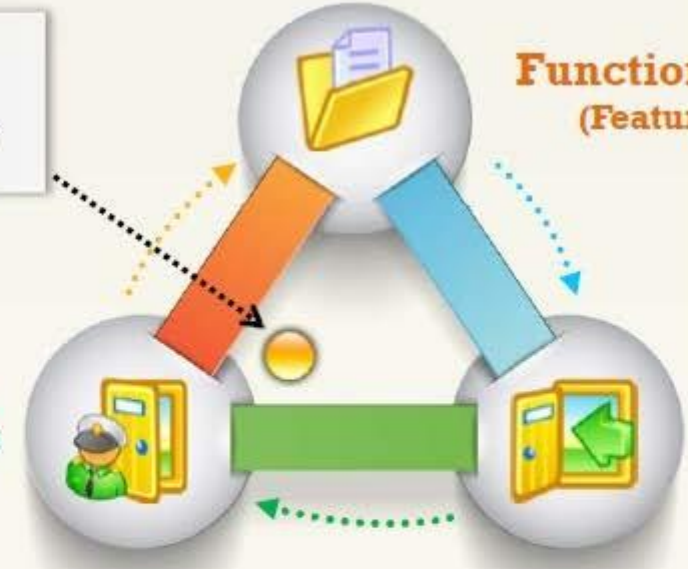
Bot

A "bot" is a software application that can be **controlled remotely to execute or automate predefined tasks**

The Security Functionality and Usability Triangle

Level of security in any system can be defined by the strength of three components:

Moving the ball towards security means less functionality and usability



Motive, Goals, and Objectives of Information Security Attacks

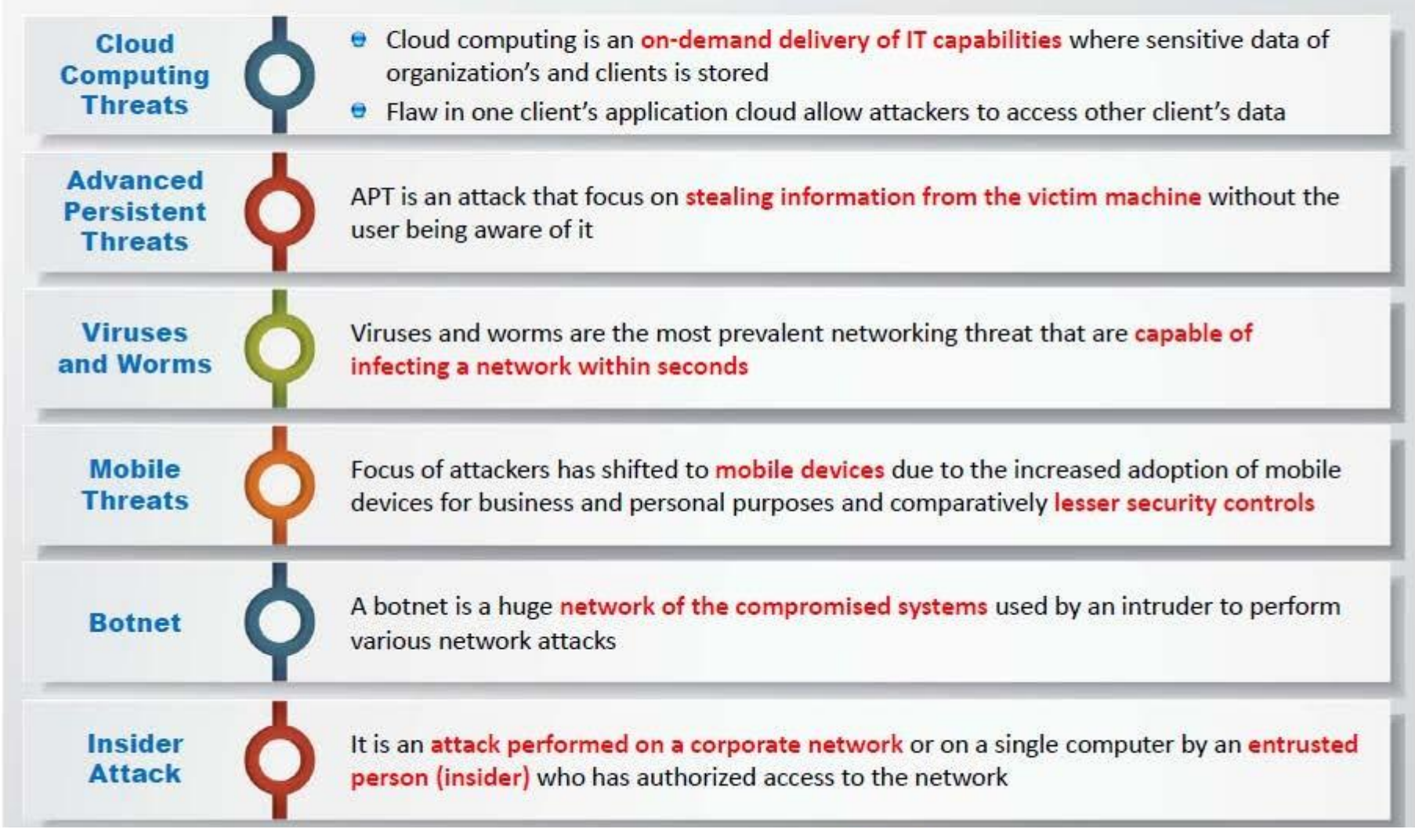
Attacks = Motive (Goal) + Method + Vulnerability

- A motive originates out of the notion that the **target system stores or processes** something valuable and this leads to threat of an attack on the system
- Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or security policy and controls to achieve their motives

Motives Behind Information Security Attacks

- Disrupting business continuity
- Information theft
- Manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Propagating religious or political beliefs
- Achieving state's military objectives
- Damaging reputation of the target
- Taking revenge

Top Information Security Attack Vectors



Information Warfare

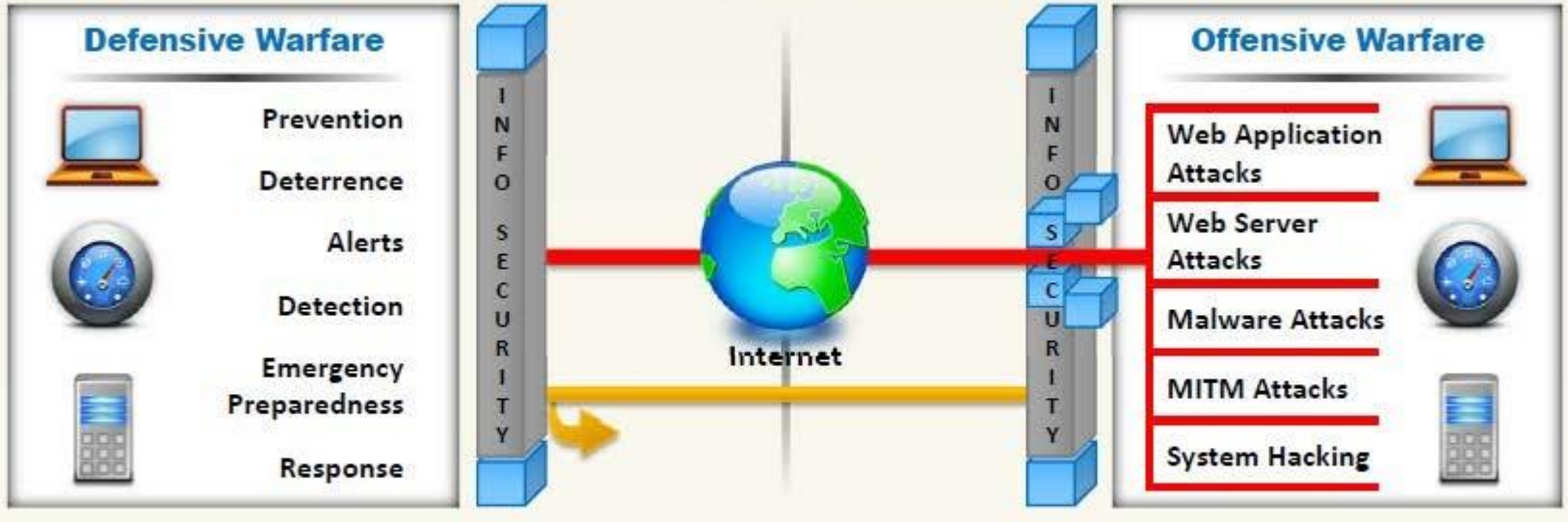
The term information warfare or InfoWar refers to the **use of information and communication technologies (ICT)** to take competitive advantages over an opponent

Defensive Information Warfare

It refers to all strategies and actions to **defend against attacks on ICT assets**

Offensive Information Warfare

It refers to information warfare that involves **attacks against ICT assets** of an opponent



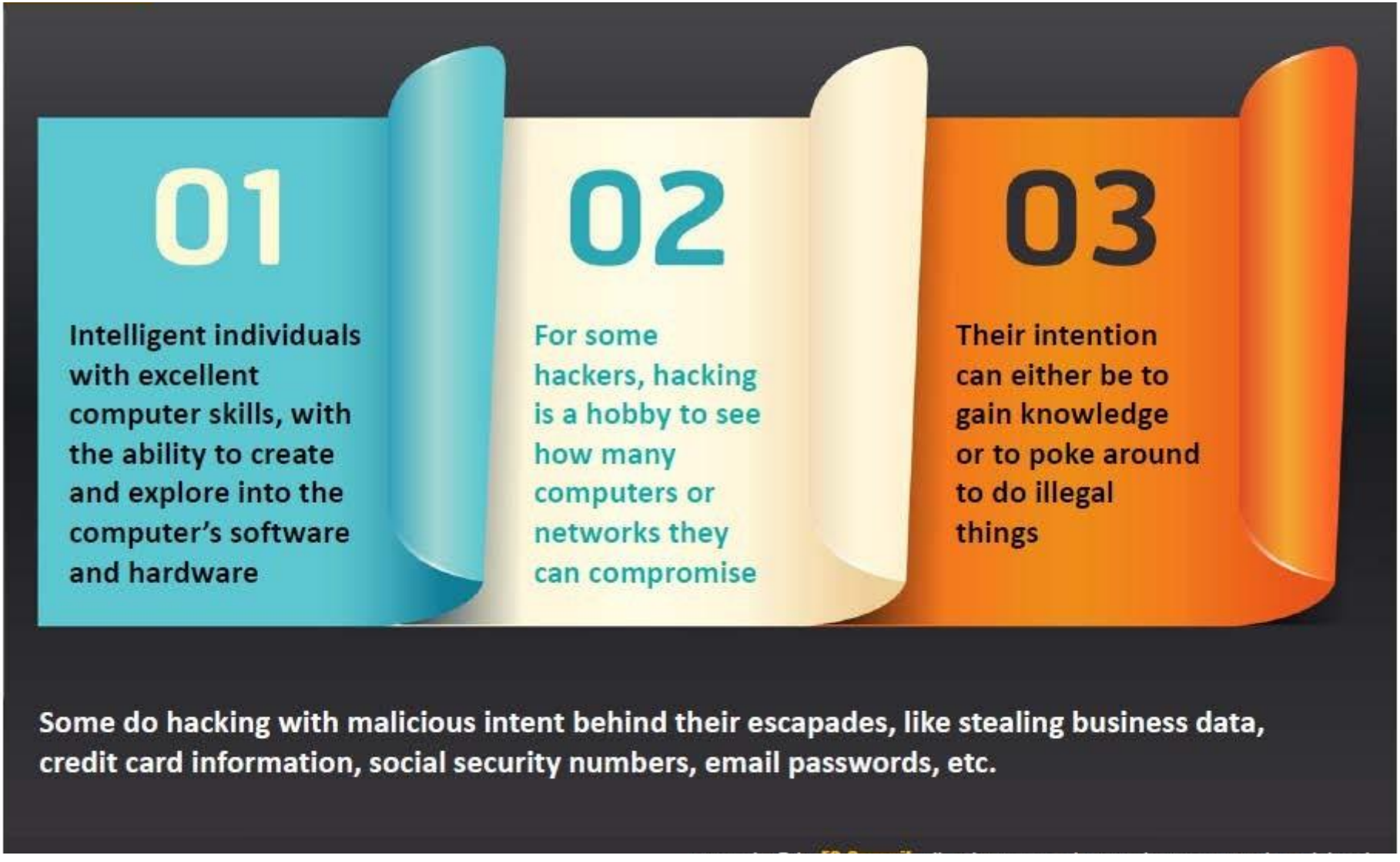
What is Hacking ??

Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to the system resources

It involves modifying system or application features to achieve a goal outside of the creator's original purpose

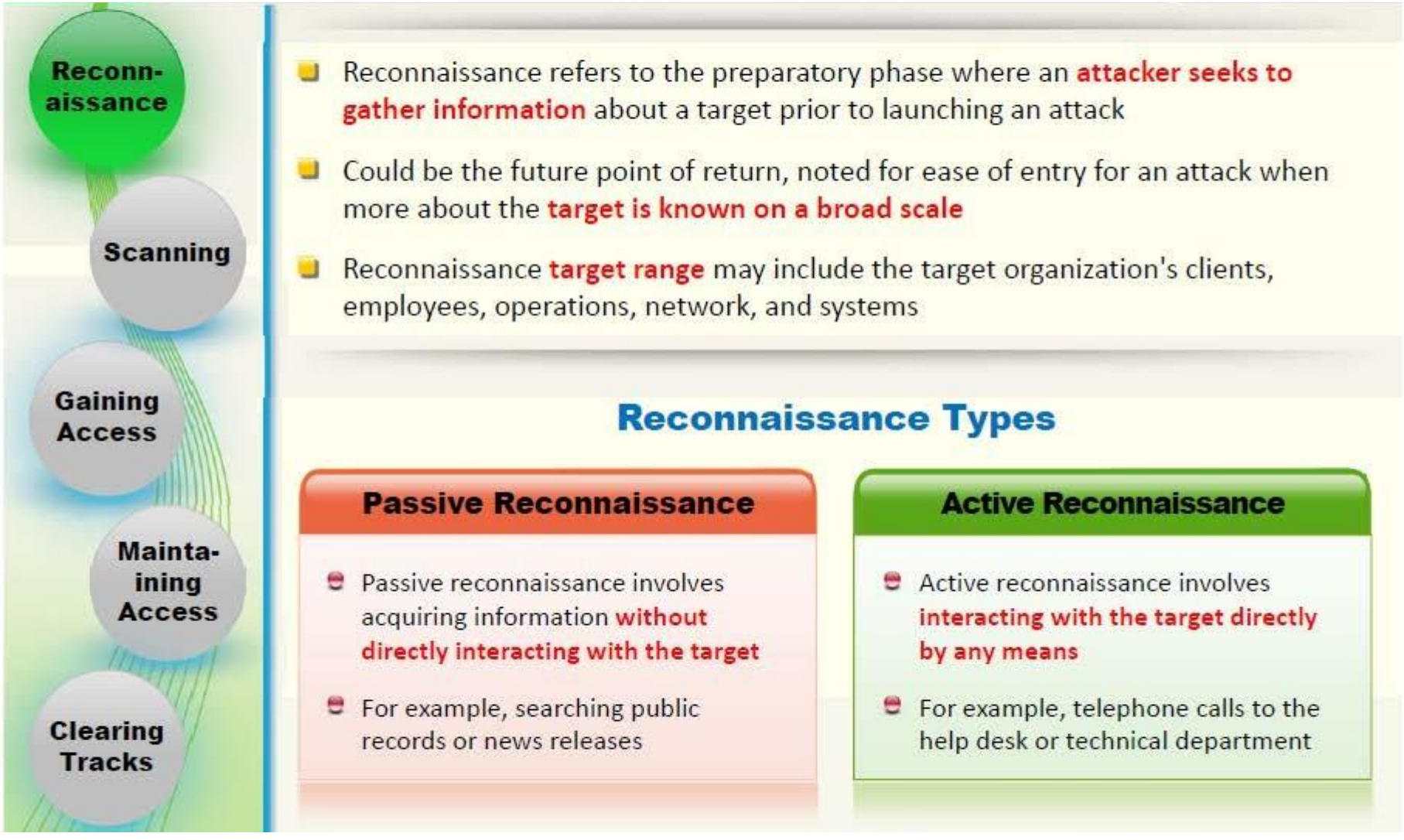
Hacking can be used to steal, pilfer, and redistribute intellectual property leading to business loss

Who is Hacker ??

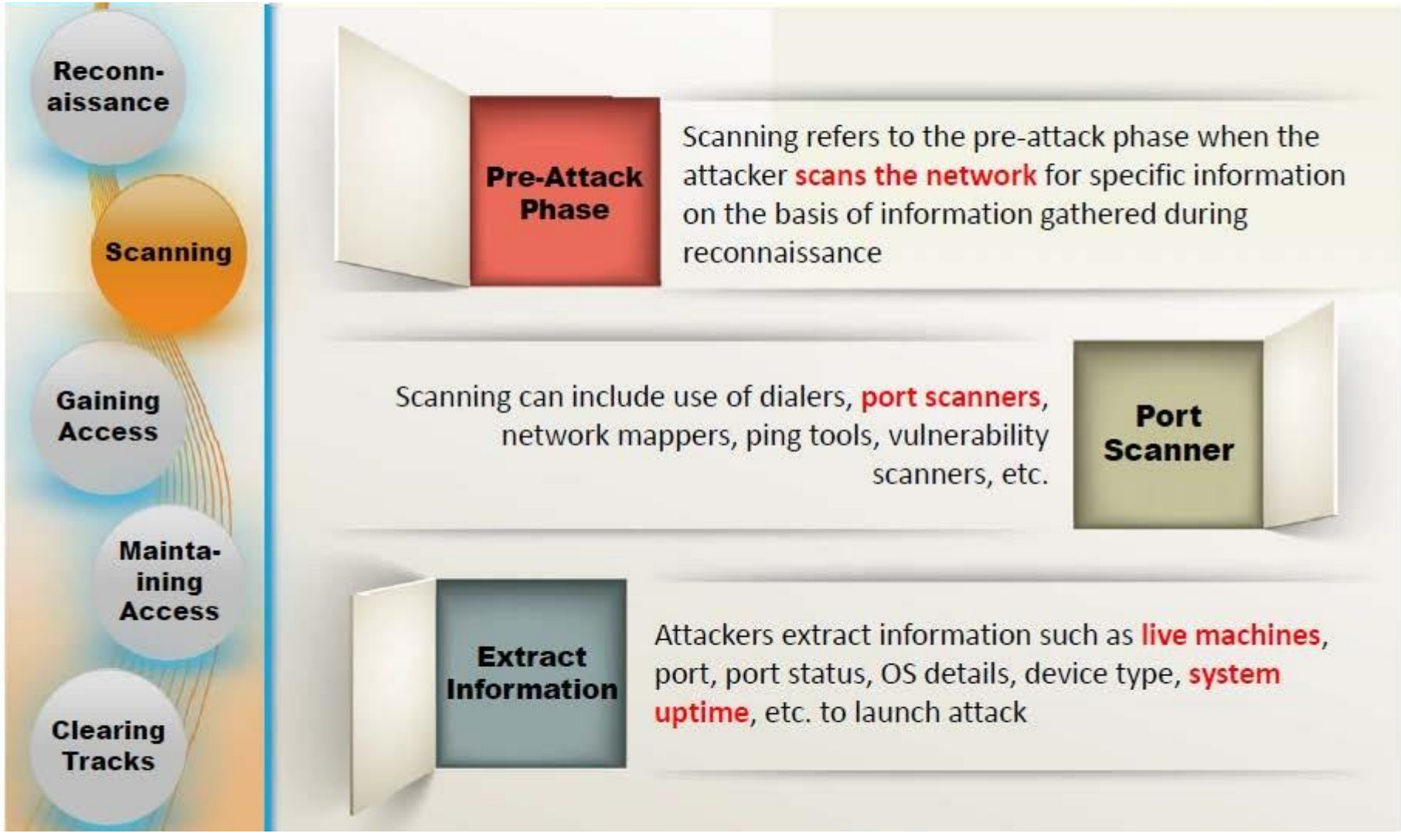


Hacker Classes

Hacking Phases: Scanning

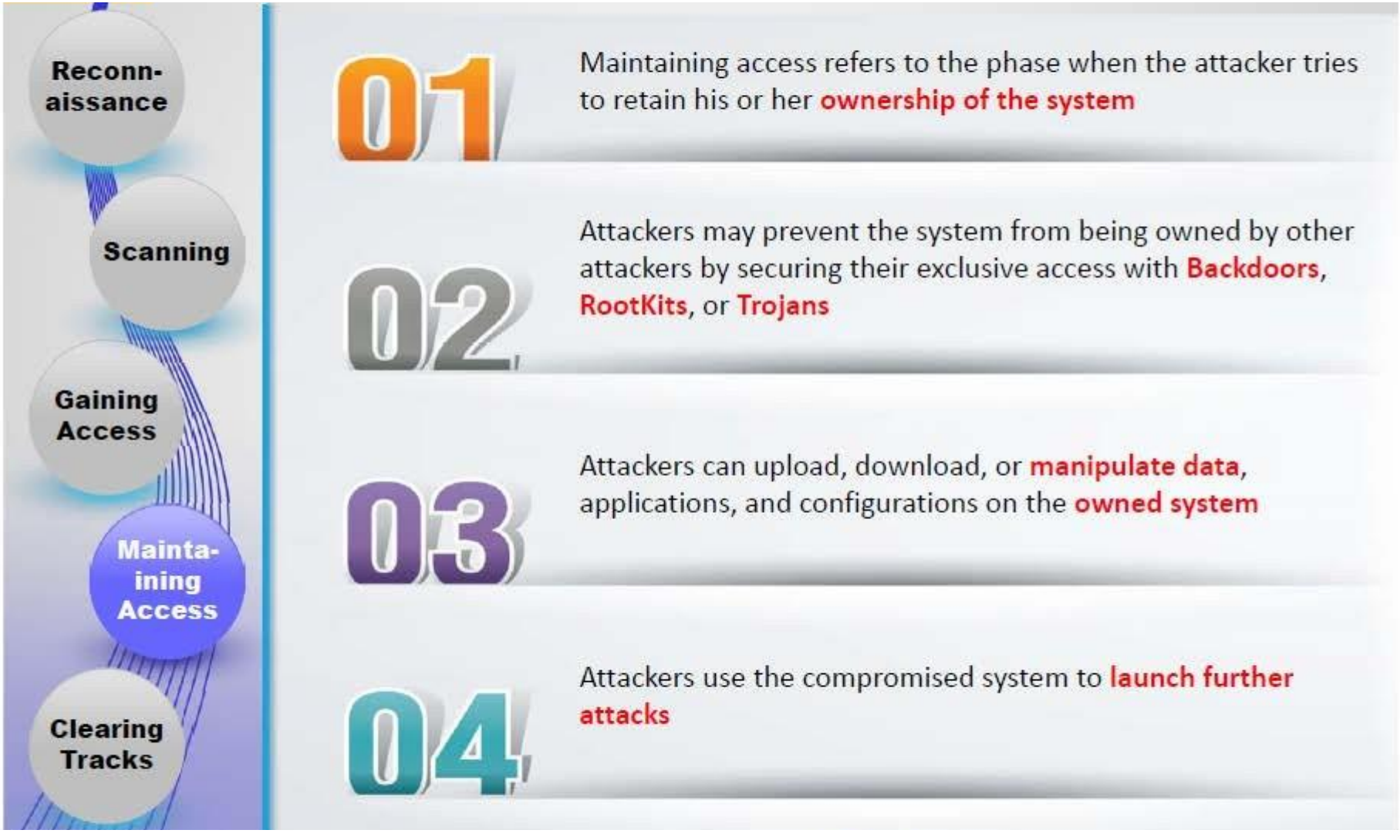


Hacking Phases: Scanning

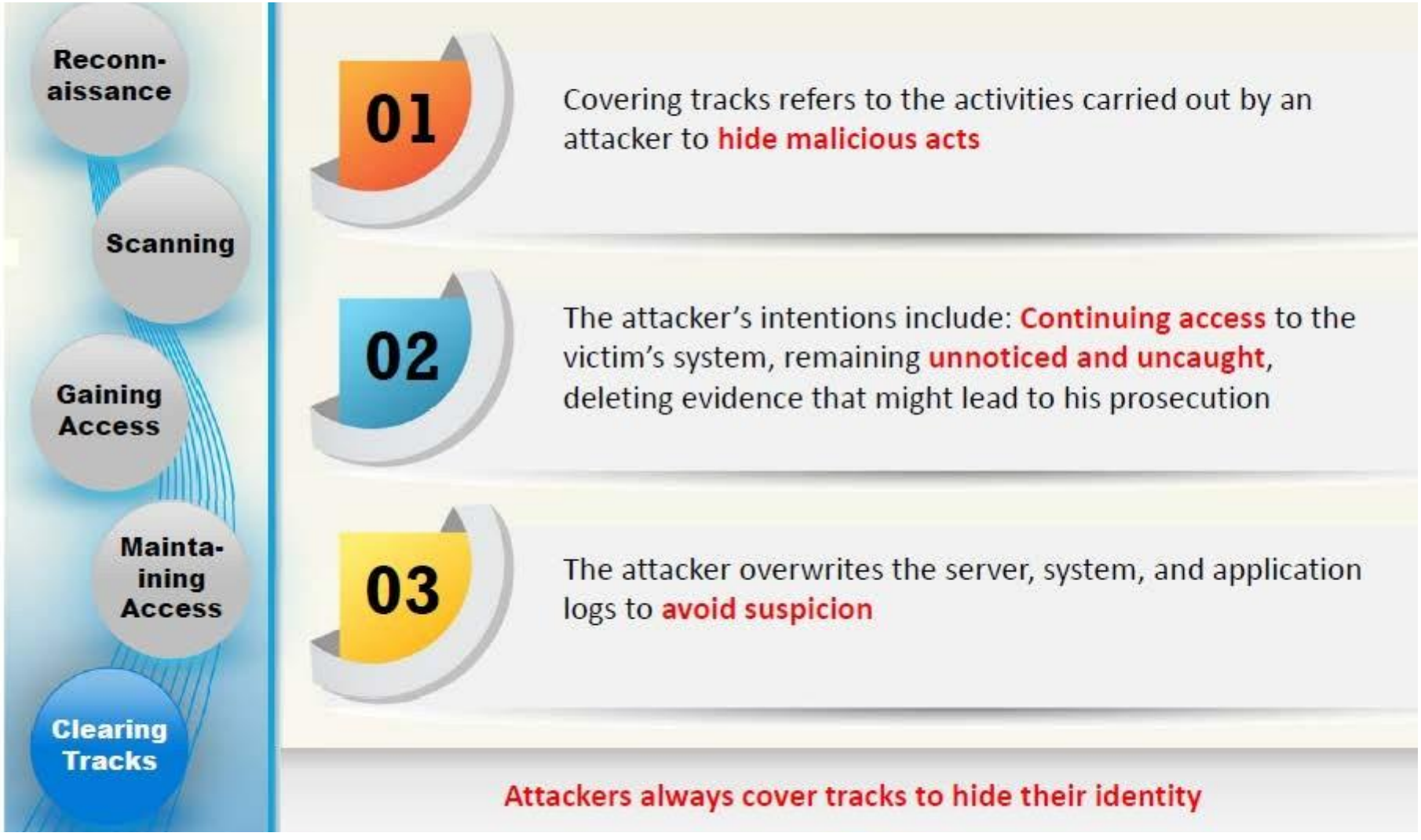


Hacking Phases: Gaining Access

Hacking Phases: Maintaining Access



Hacking Phases: Clearing Tracks



What is Ethical Hacking ??

Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** so as to ensure system security

It focuses on simulating techniques used by attackers to **verify the existence of exploitable vulnerabilities** in the system security

Ethical hackers performs security assessment of their organization **with the permission of concerned authorities**

Why an Ethical Hacker is Necessary

To beat a hacker, you need to think like one!

Ethical hacking is necessary as it **allows to counter attacks from malicious hackers** by anticipating methods used by them to break into a system

Reasons why Organizations Recruit Ethical Hackers

To **prevent hackers** from gaining access to organization's information systems

To **uncover vulnerabilities** in systems and explore their potential as a risk

To analyze and **strengthen an organization's security posture** including policies, network protection infrastructure, and end-user practices

Why an Ethical Hacker is Necessary

Ethical Hackers Try to Answer the Following Questions

What can the intruder see on the **target system**? (Reconnaissance and Scanning phases)

What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)

Does anyone at the target **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)

If all the **components of information system** are adequately protected, updated, and patched

How much effort, time, and money is required to obtain **adequate protection**?

Are the **information security measures** in compliance to industry and legal standards?

Skills of an Ethical Hacker

1 Technical Skills

- Has in-depth **knowledge of major operating environments**, such as Windows, Unix, Linux, and Macintosh
- Has in-depth **knowledge of networking** concepts, technologies and related hardware and software
- Should be a **computer expert** adept at technical domains
- Has **knowledge of security areas** and related issues
- Has "**high technical**" **knowledge** to launch the sophisticated attacks

2 Non-Technical Skills

Some of the non-technical characteristics of an ethical hacker include:

- **Ability to learn** and adapt new technologies quickly
- **Strong work ethics**, and good problem solving and communication skills
- Committed to **organization's security policies**
- Awareness of **local standards and laws**

Online Security Recourse

CERT

www.cert.org

Microsoft Security Advisor

www.microsoft.com/security/default.mspx

F-Secure

www.f-secure.com

SANS

www.sans.org