

Introducing myself

Dr. Zakria

PhD, Software Engineering

University of Electronic Science and Technology of China.

MS, Computer Science and Information Technology

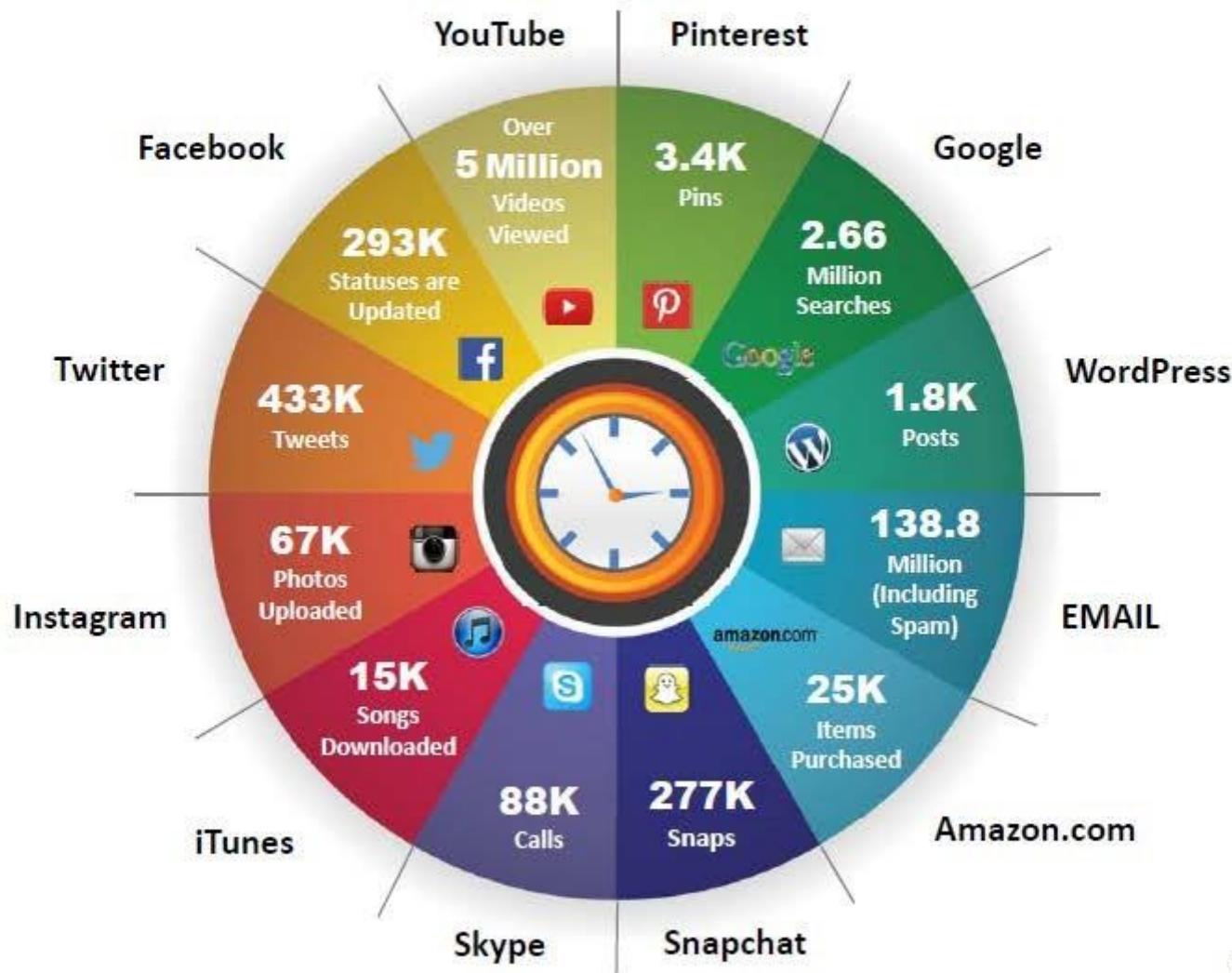
NED University of Engineering and Technology, Karachi.

BS, Computer Engineering

COMSATS University, Lahore, Pakistan

Internet is Integral part of business and personal life

What happens online in 60 seconds



Case Study : Ebay data breach



Records of **145 million** user were compromised

Records contained **passwords, email addresses, birth dates, mailing addresses** and other personal information



Case Study : Google Play Hack



A Turkish hacker has brought down **Google Play's entire system** twice, preventing any downloads or uploads to it



The hacker uploaded a **malformed APK** to **Android app database** to test a vulnerability in the application. This caused **Denial of Service on Google Play!**

Case Study : The Home Depot data breach

56 million debit and credit
card numbers were stolen



Incident occurred due
to **custom-built
malware**

Case Study : JP Morgan Chase data breach

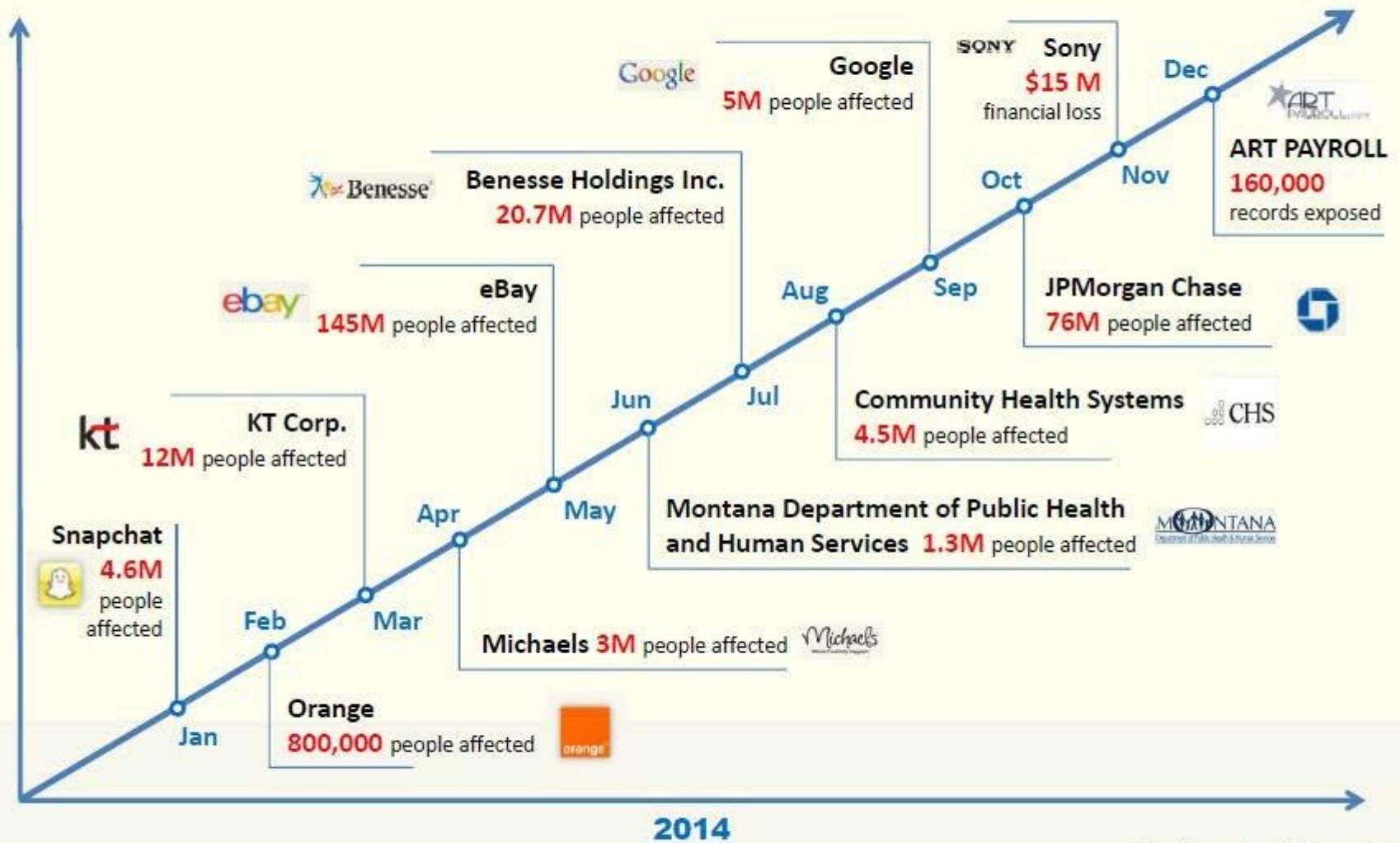
Contact information for **76 million households** and **7 million small businesses** were compromised

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

JPMorganChase

<http://dealbook.nytimes.com>

Case Study : Year of Mega Breaches

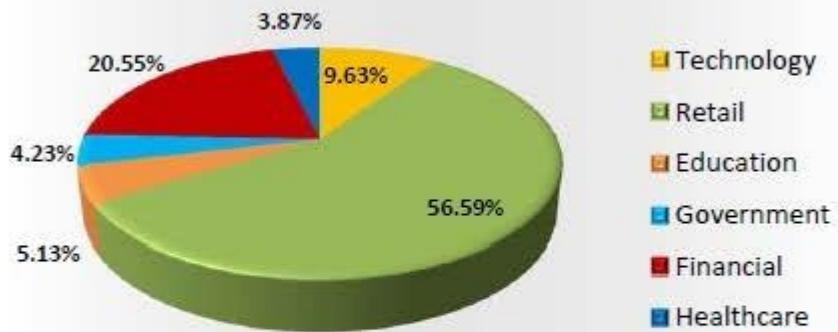


Data Breach Statistics

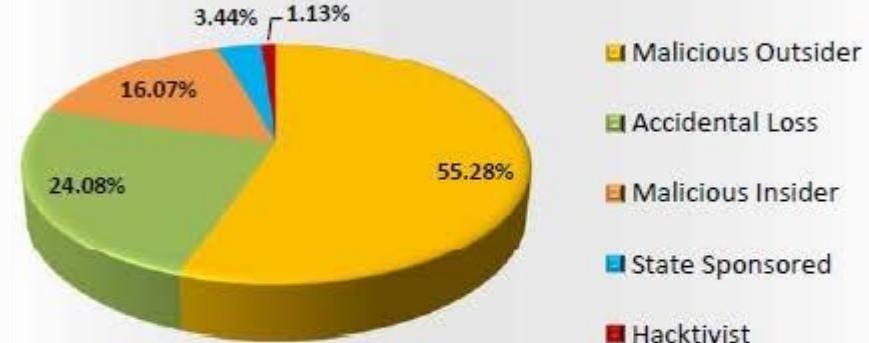
There were over **3,007,682,404** data records lost or stolen since 2013 till Mar-2015



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?

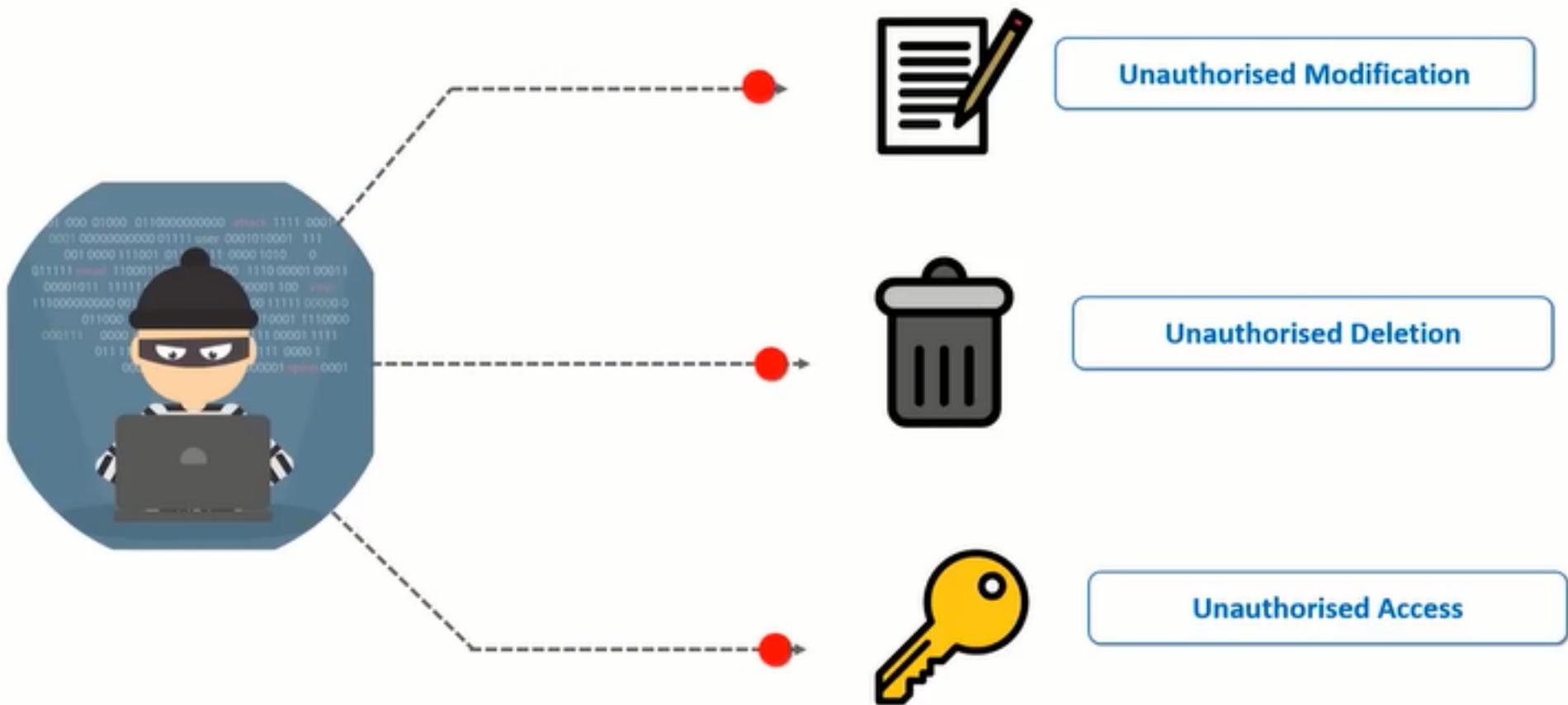
Cyber security is the protection of Internet connected system, including hardware, software, and program or data from cyber attacks.

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

Activate Windows
Go to Settings to activate Window

Types of Attacks

Malware



01

Phishing



02

Password Attacks



03

DDoS



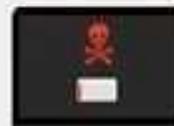
04

Man in the Middle



05

Drive-By Download



06

Malvertising



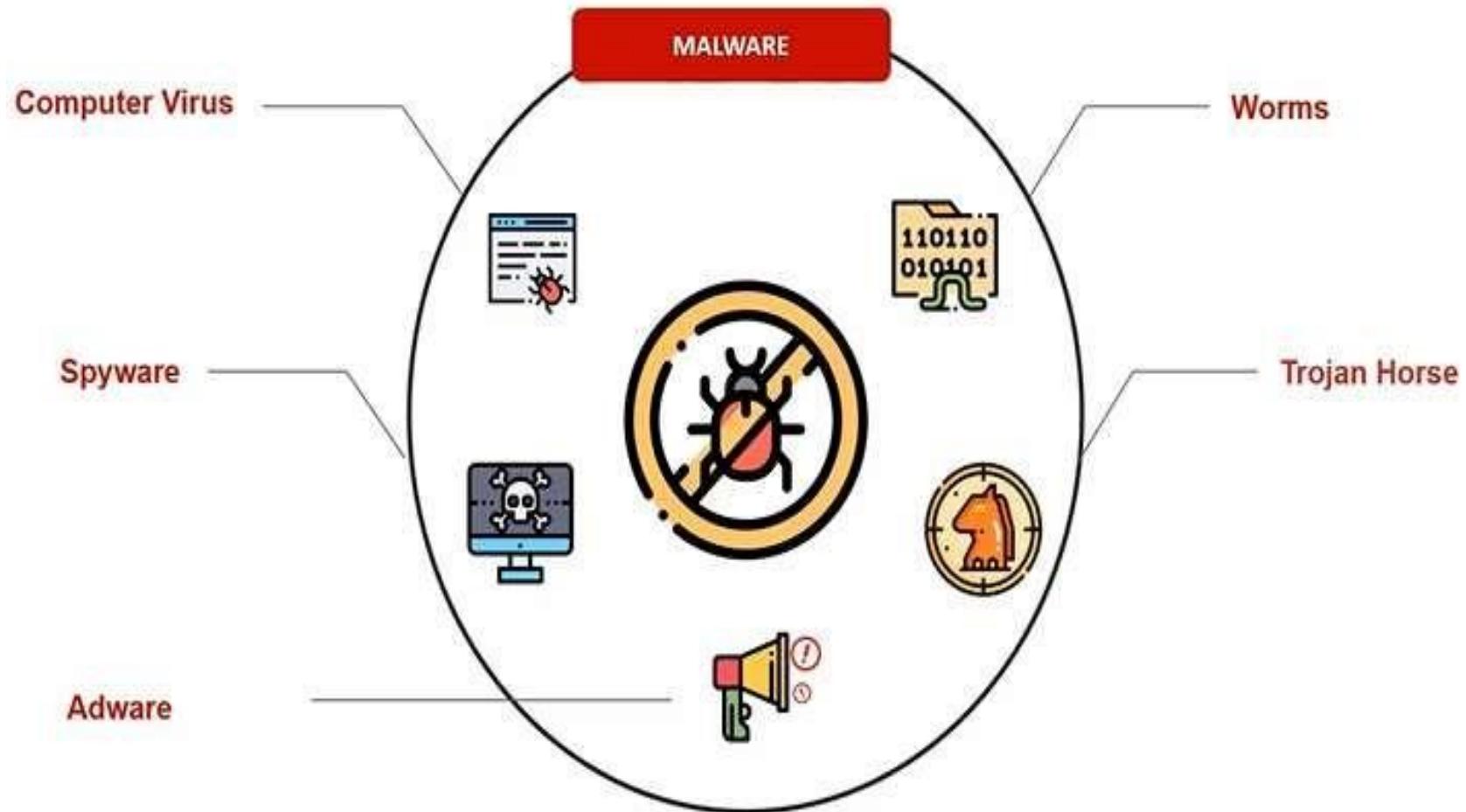
07

Rogue Software



08

Malware



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

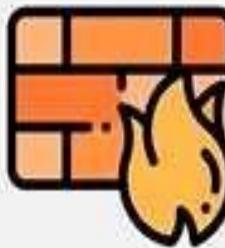
How to Stop?

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



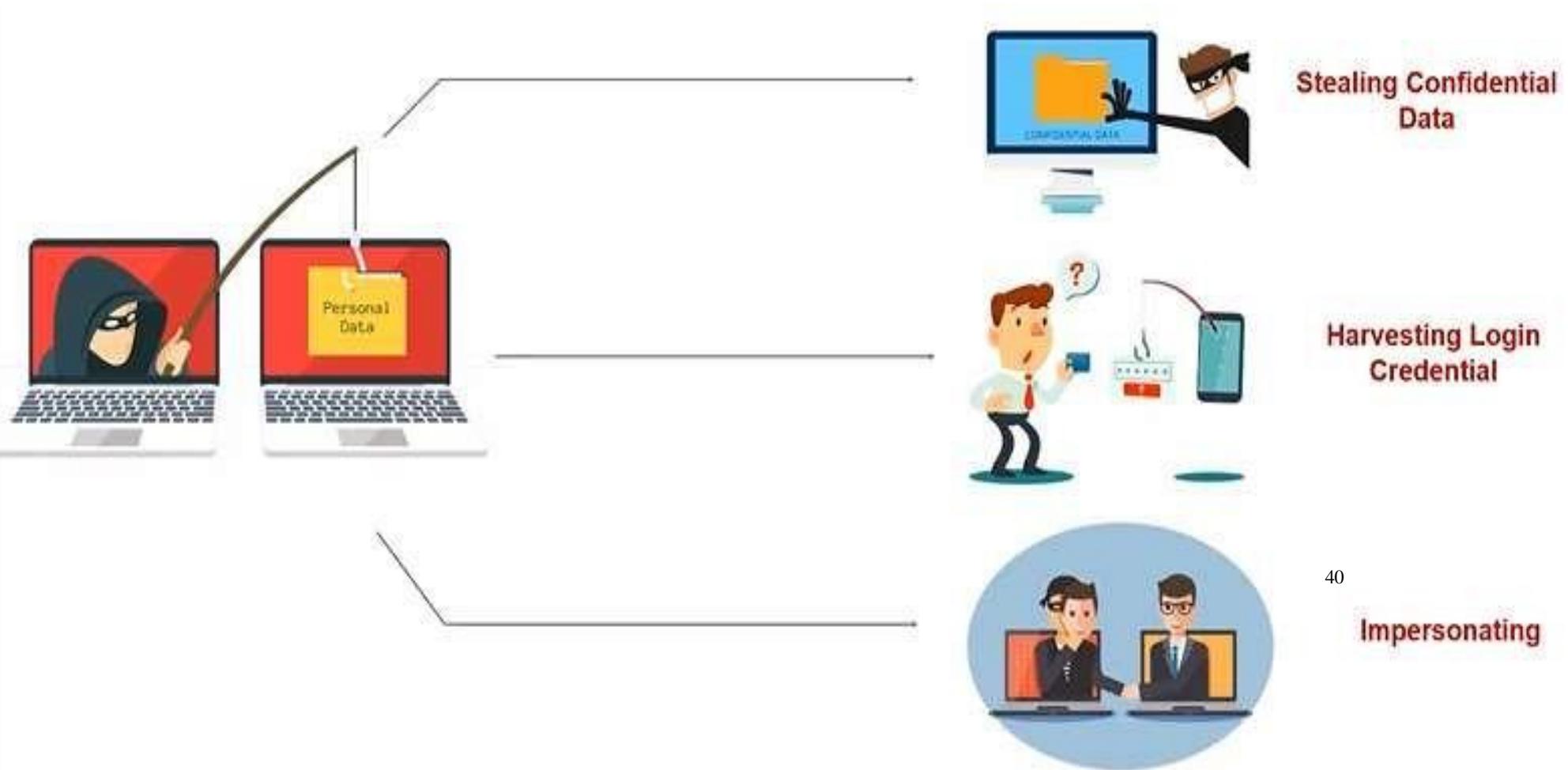
- It's also important to make sure your computer's operating system (e.g. Windows, Mac OS X, Linux) uses the most up-to-date security updates
- Software programmers update programs frequently to address any holes or weak points.

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?



Phishing Awareness

Always check the sender email address

The image shows a simulated email inbox with a single message from 'Amazon<management@mazoncanada.ca>' with the subject 'Account Detail Compromised'. The message body contains a warning about account compromise and a link to click here to unlock the account. The signature at the bottom is from the 'Amazon Associate Team'.

From: Amazon<management@mazoncanada.ca>

Subject: Account Detail Compromised

amazon.com

Dear client,

We have strong reasons to believe that your credentials may have been compromised and might have been used by someone else. We have locked your amazon account please [click here](#) to unlock.

Sincerely,
Amazon Associate Team

Reply 0

Look out for common generalised addressing

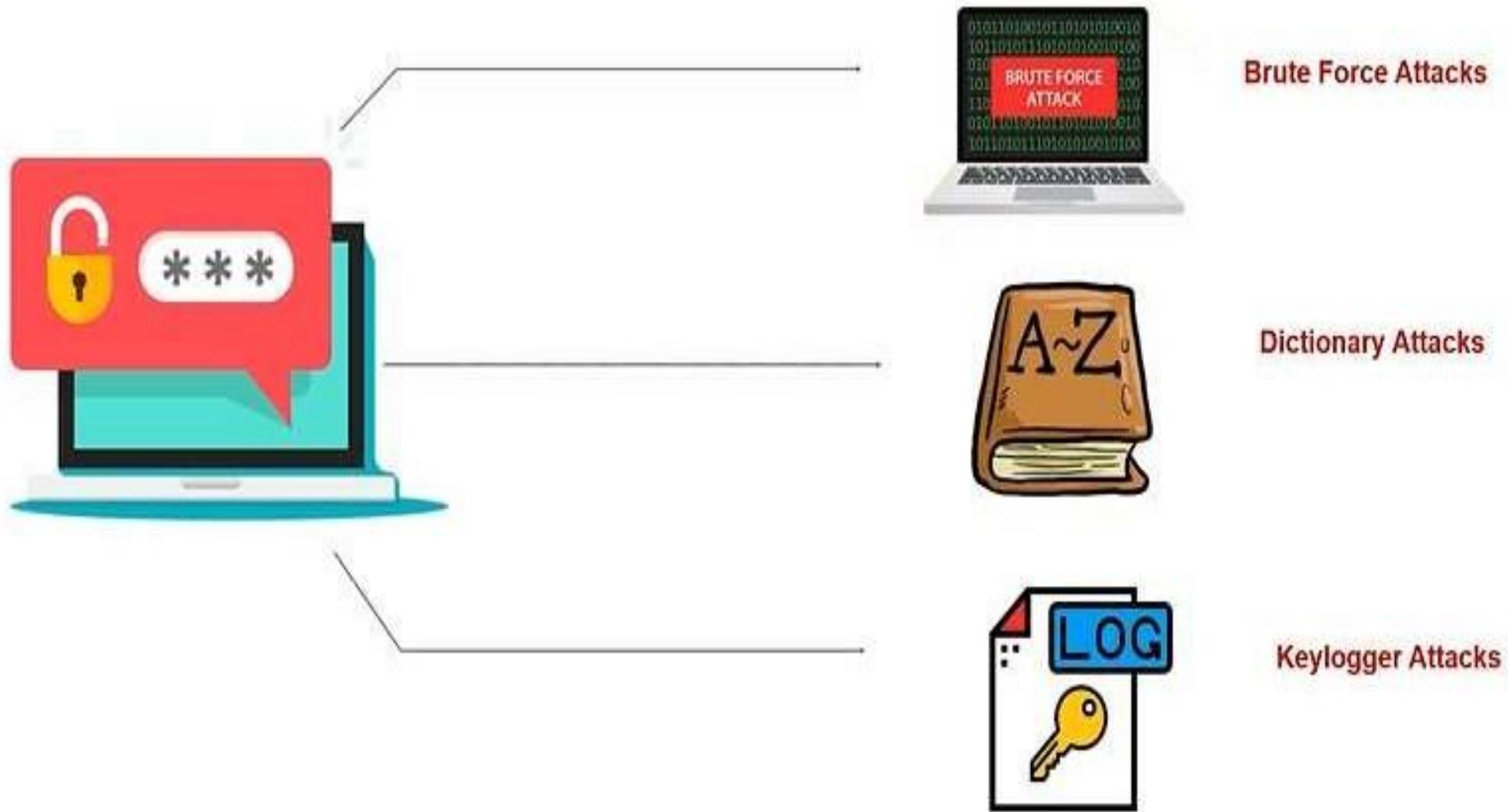
Always hover over links to check the redirect address

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



Password Attack



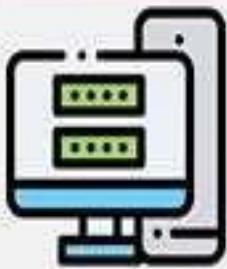
1234, XYZ
ABCD, 3210



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



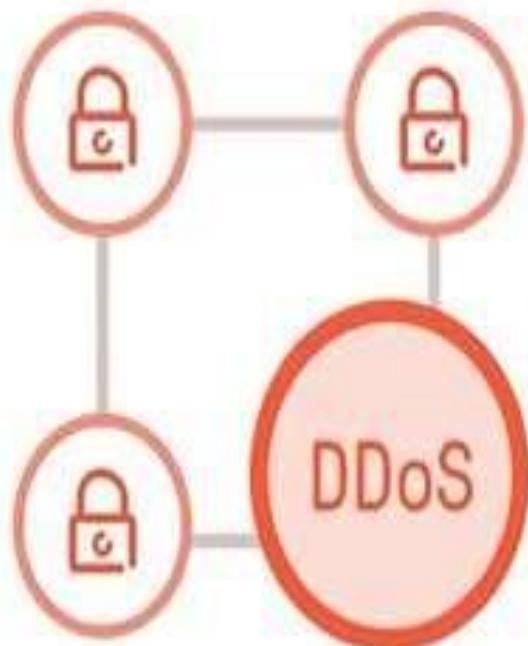
- When setting a password general best practices should be followed
- A password should contain a multitude of characters with a generous use of alpha numeric

NO Dictionary



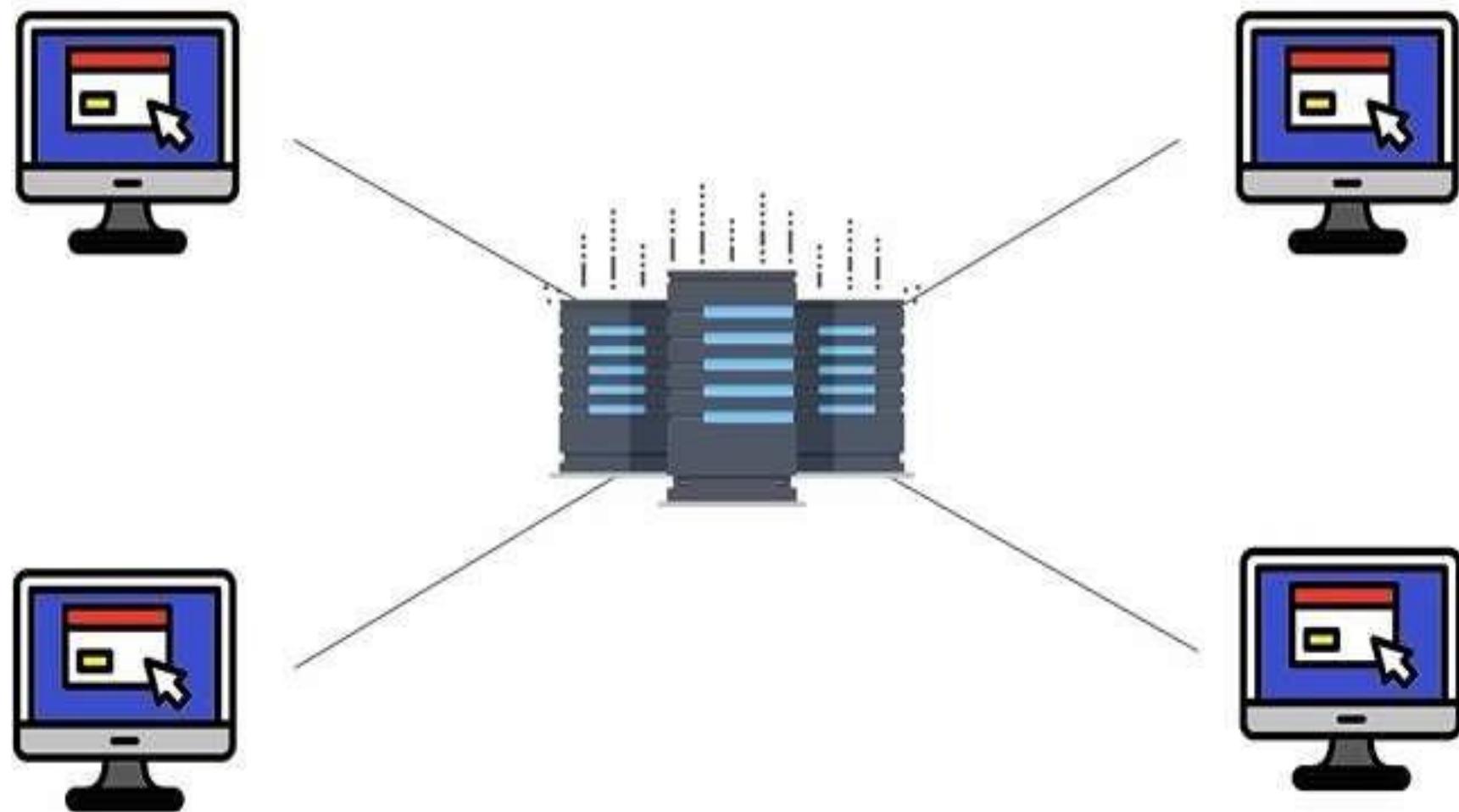
- It's always a great idea to use a password that only makes sense to you
- Passwords which use actual words that make sense are much more susceptible to dictionary attacks

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

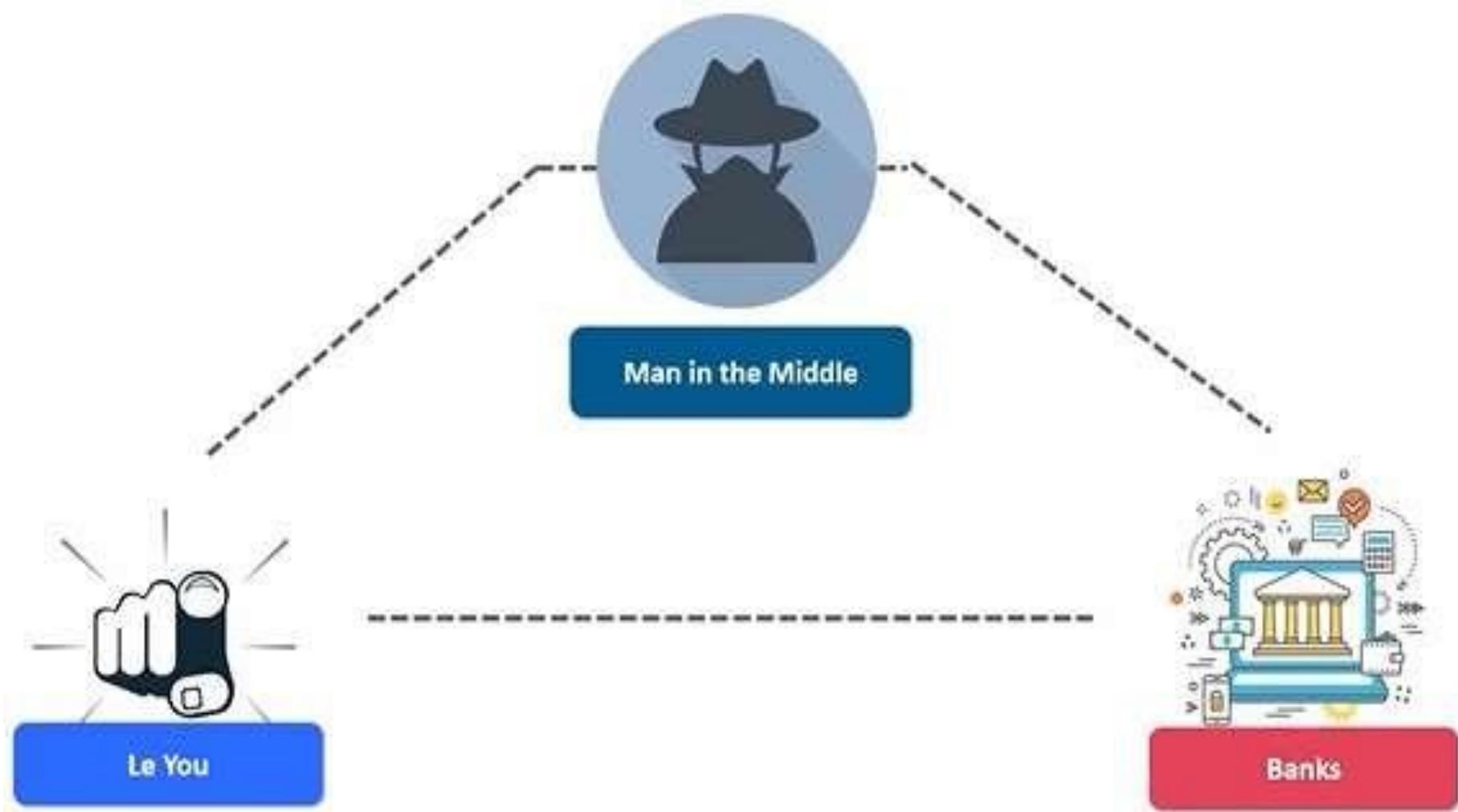
Traffic Analysis

Traffic Control

Recovery
Management



Man in the Middle



Prevent MITM

Use encrypted WAP

Always check the security of your 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.⁵⁰

How it work?

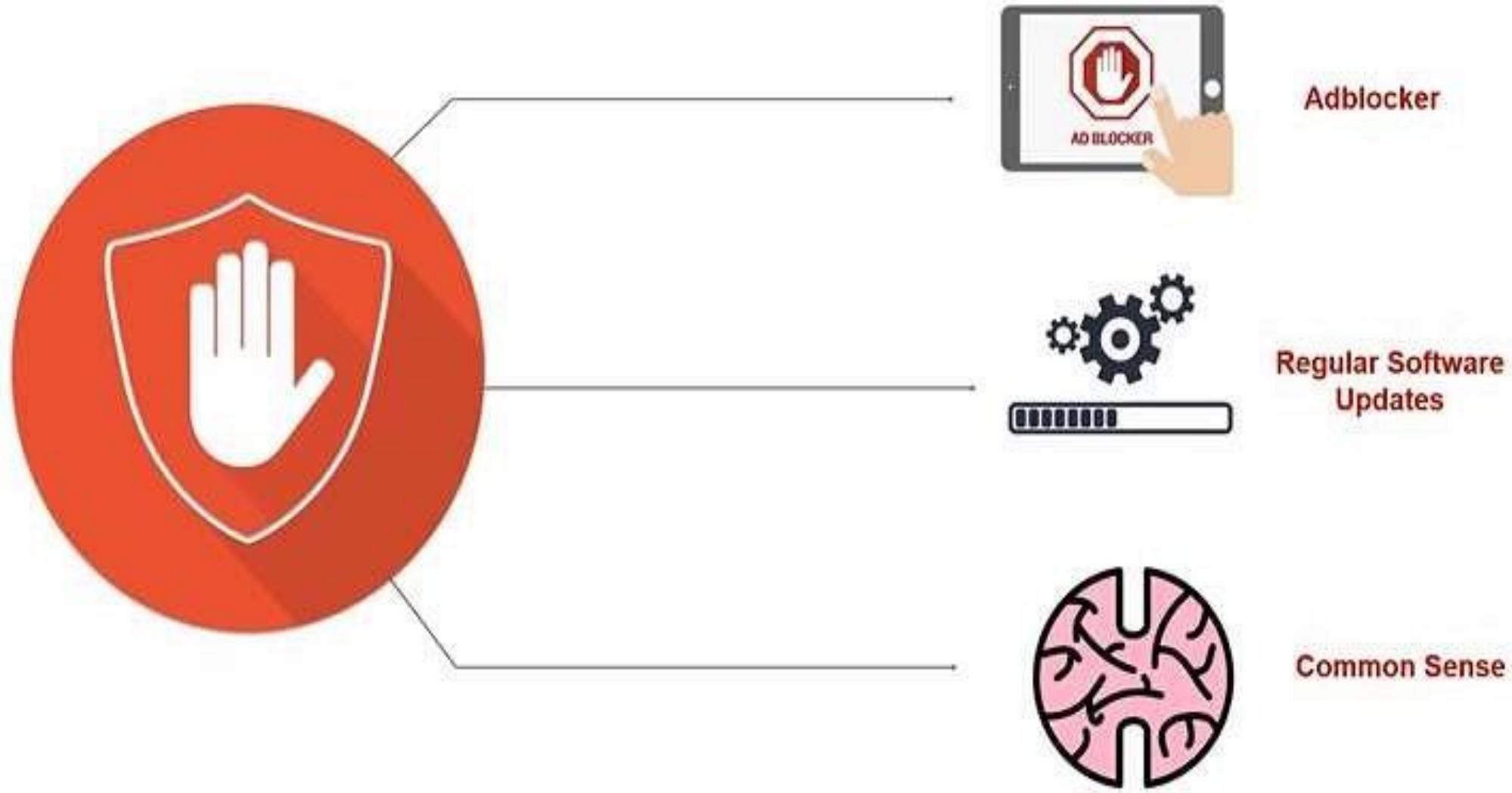


Malvertising

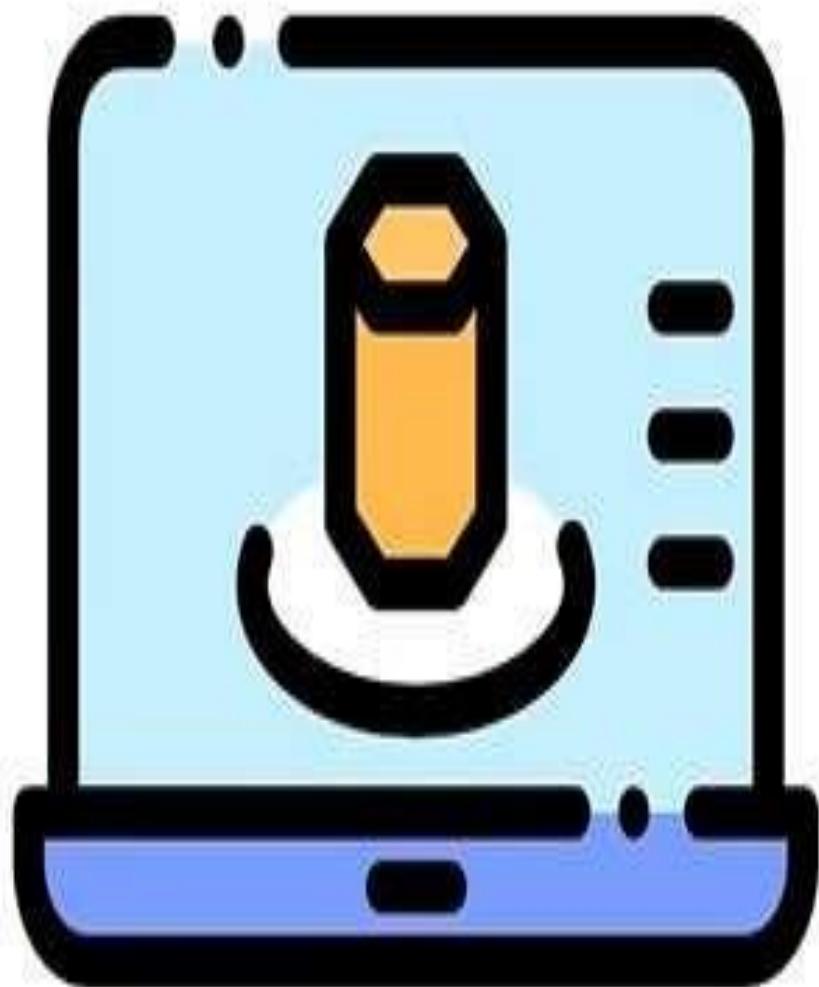
Malvertising is the name we in the security industry give to criminally-controlled adverts which intentionally infect people and businesses. These can be any ad on any site – often ones which you use as part of your everyday Internet usage. It is a growing problem, as is evidenced by a recent US Senate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



Prevention



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

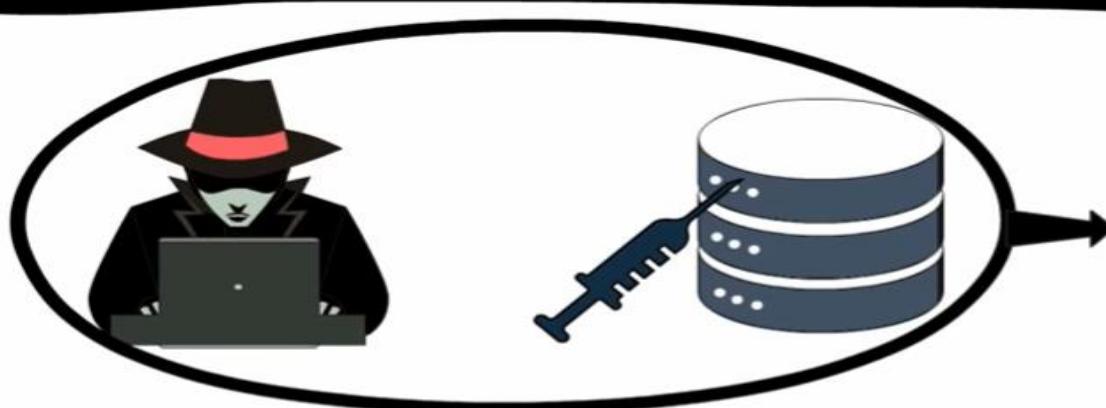


SQL injection

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

1	ABC	123	12/01/2019
2	XYZ	456	20/03/2019
3	ABC	123	12/01/2019
4	XYZ	456	20/03/2019
5			
6			
7			
8			

The table illustrates a database structure with four columns. The first column contains row numbers (1-8). The second column contains values 'ABC' (rows 1, 3), 'XYZ' (rows 2, 4), and empty cells (rows 5-8). The third column contains values '123' (rows 1, 3, 5), '456' (rows 2, 4, 6), and empty cells (rows 7, 8). The fourth column contains dates '12/01/2019' (rows 1, 3, 7), '20/03/2019' (rows 2, 4, 8), and empty cells (rows 5, 6). Overlaid on the table are several icons: a magnifying glass over the first row, a pencil over the second row, and a trash can over the eighth row.

DNS Poisoning

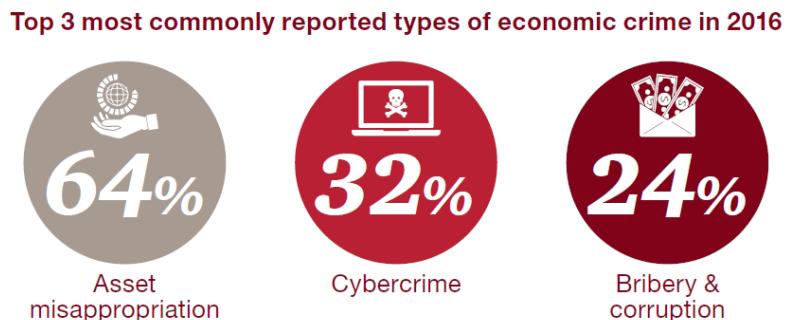
This involves altering DNS records on a DNS server to redirect client traffic to malicious websites, usually for identity theft.



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 reported by the [2013 Europol Serious & Organized Threat Assessment](#), the “Total Global Impact of CyberCrime [has risen to] US \$3 Trillion, making it more profitable than the global trade in marijuana, cocaine and heroin combined.”

MEDIA CORNER

- Europol Media Corner
- Press releases
- News
- Events

Home > Media Corner > Corporate Publications > EU Serious and Organised Crime Threat Assessment (SOCTA 2013)

Print friendly page | Print as PDF

Shares:

EU SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA 2013)

19 March 2013

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 steal 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

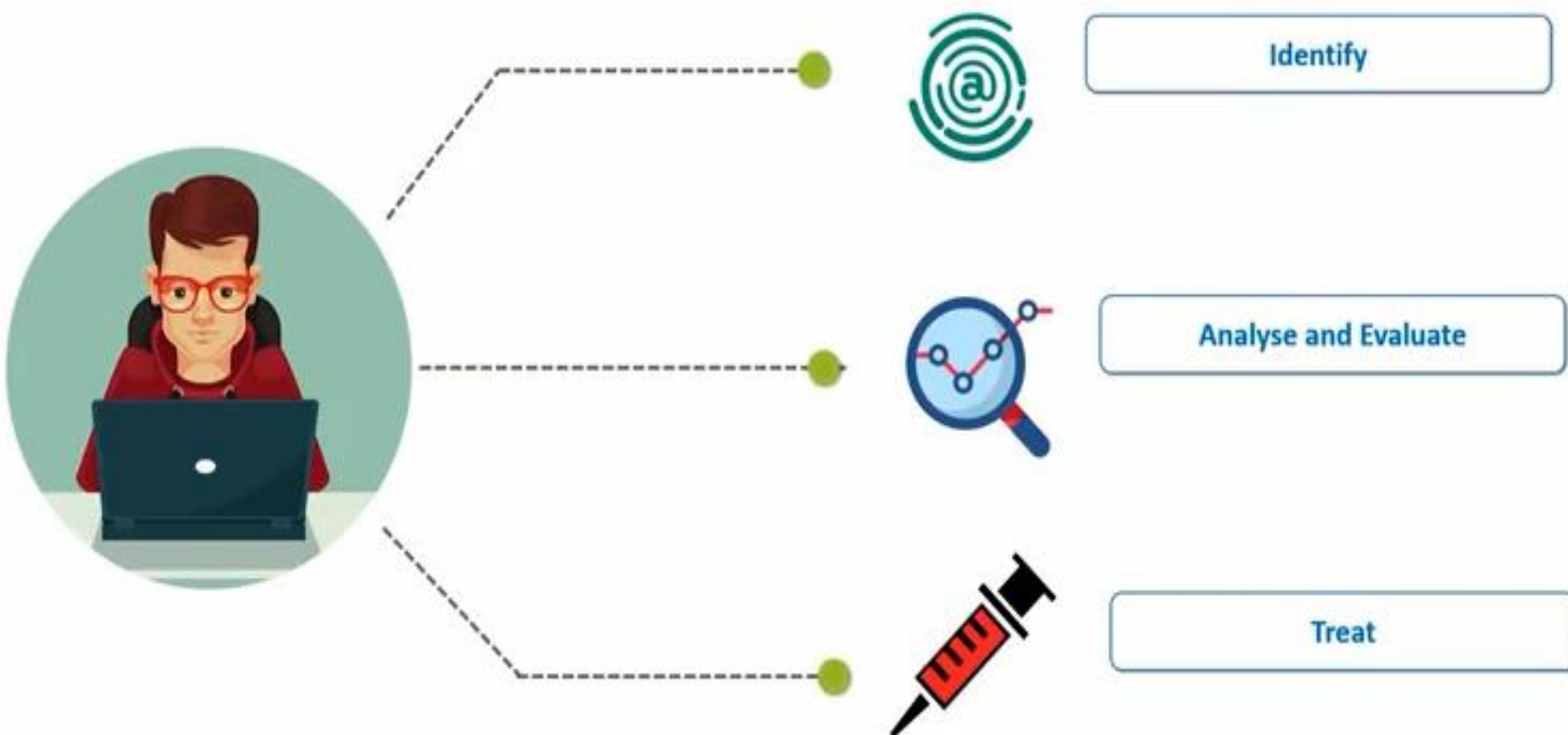
Cross Site Scripting

- 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

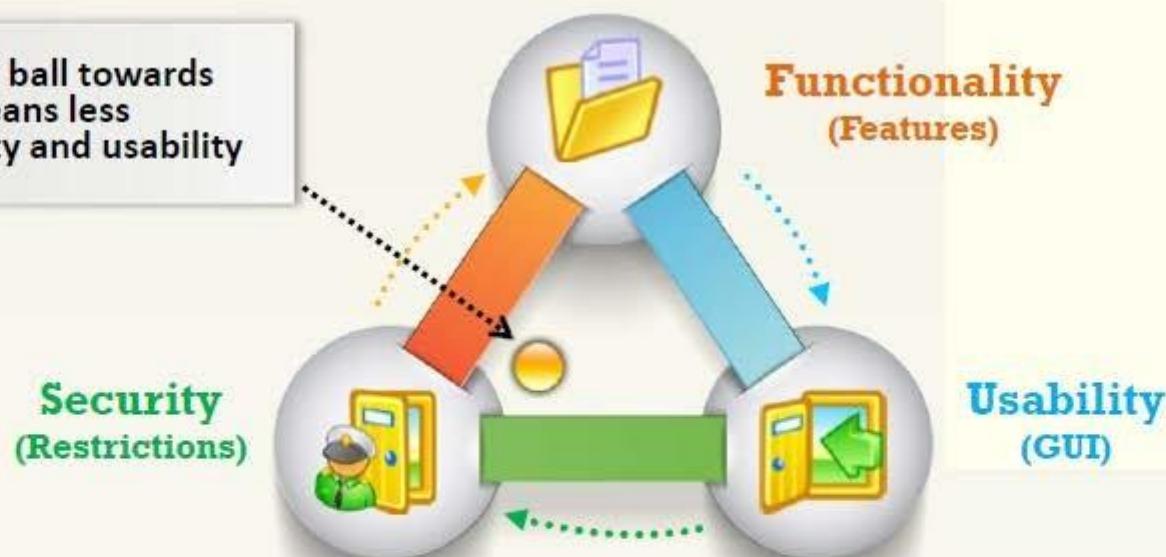
A “bot” is a software application that can be **controlled remotely to execute or automate predefined tasks**

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

Cloud Computing Threats		<ul style="list-style-type: none">Cloud computing is an on-demand delivery of IT capabilities where sensitive data of organization's and clients is storedFlaw in one client's application cloud allow attackers to access other client's data
Advanced Persistent Threats		APT is an attack that focus on stealing information from the victim machine without the user being aware of it
Viruses and Worms		Viruses and worms are the most prevalent networking threat that are capable of infecting a network within seconds
Mobile Threats		Focus of attackers has shifted to mobile devices due to the increased adoption of mobile devices for business and personal purposes and comparatively lesser security controls
Botnet		A botnet is a huge network of the compromised systems used by an intruder to perform various network attacks
Insider Attack		It is an attack performed on a corporate network or on a single computer by an entrusted person (insider) who has authorized access to the network

Information Warfare

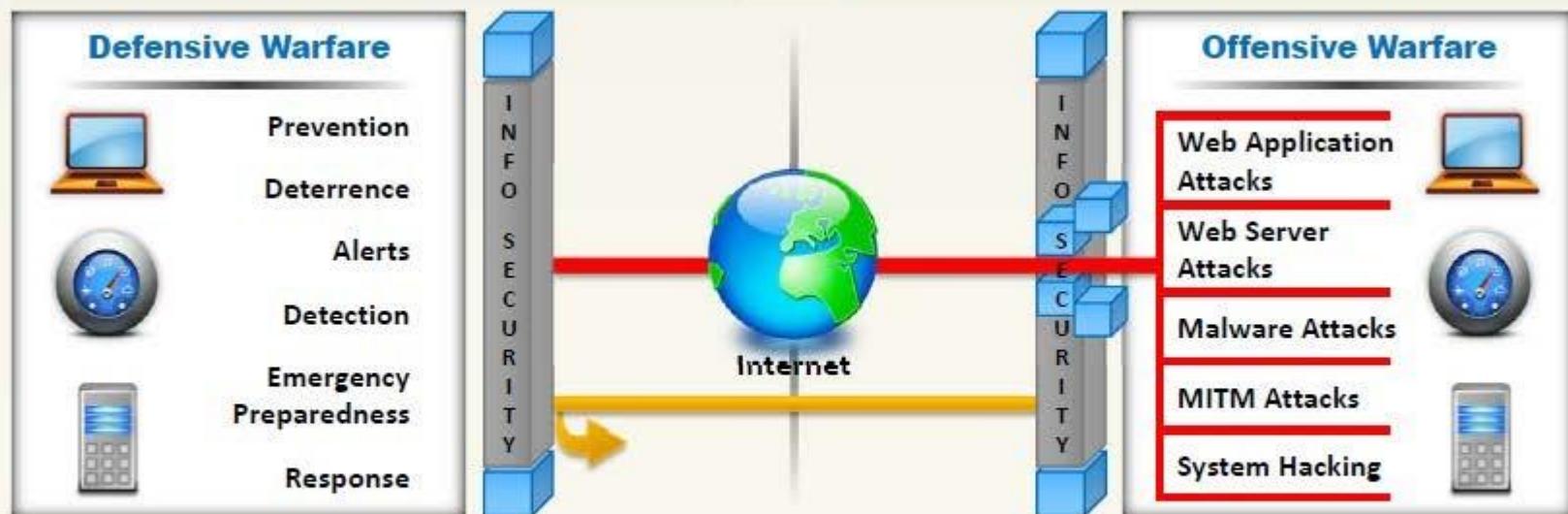
The term information warfare or InfoWar refers to the **use of information and communication technologies (ICT)** to take competitive advantages over an opponent

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 ??

01

Intelligent individuals with excellent computer skills, with the ability to create and explore into the computer's software and hardware

02

For some hackers, hacking is a hobby to see how many computers or networks they can compromise

03

Their intention can either be to gain knowledge or to poke around to do illegal things

Some do hacking with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.

Hacker Classes

1

Black Hats

Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers

2

White Hats

Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts

3

Gray Hats

Individuals who work both offensively and defensively at various times

4

Suicide Hackers

Individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

5

Script Kiddies

An unskilled hacker who compromises system by running scripts, tools, and software developed by real hackers

6

Cyber Terrorists

Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks

7

State Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments

8

Hacktivist

Individuals who promote a political agenda by hacking, especially by defacing or disabling websites

Hacking Phases: Scanning

The diagram features five circular nodes arranged vertically on the left side, connected by green lines. The nodes are labeled from top to bottom: 'Reconnais-sance' (in a green circle), 'Scanning' (in a grey circle), 'Gaining Access' (in a light blue circle), 'Maintain-ing Access' (in a grey circle), and 'Clearing Tracks' (in a light blue circle).

- Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack
- Could be the future point of return, noted for ease of entry for an attack when more about the **target is known on a broad scale**
- Reconnaissance **target range** may include the target organization's clients, employees, operations, network, and systems

Reconnaissance Types

Passive Reconnaissance

- Passive reconnaissance involves acquiring information **without directly interacting with the target**
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves **interacting with the target directly by any means**
- For example, telephone calls to the help desk or technical department

Hacking Phases: Scanning



Pre-Attack Phase

Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information on the basis of information gathered during reconnaissance

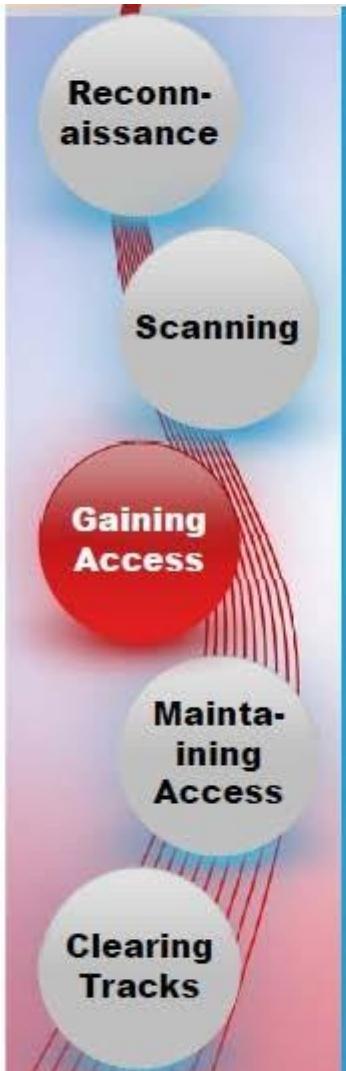
Port Scanner

Scanning can include use of dialers, **port scanners**, network mappers, ping tools, vulnerability scanners, etc.

Extract Information

Attackers extract information such as **live machines**, port, port status, OS details, device type, **system uptime**, etc. to launch attack

Hacking Phases: Gaining Access



Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the computer or network



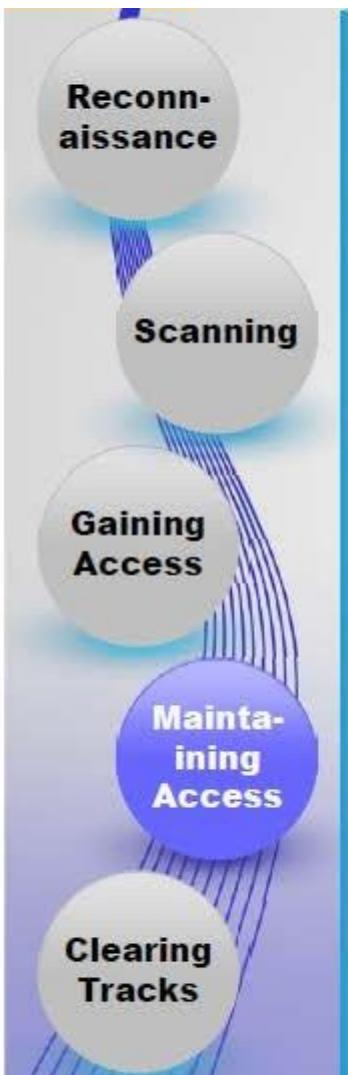
The attacker can **escalate privileges** to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised

The attacker can gain access at the **operating system level, application level, or network level**



Examples include **password cracking**, buffer overflows, denial of service, **session hijacking**, etc.

Hacking Phases: Maintaining Access



01

Maintaining access refers to the phase when the attacker tries to retain his or her **ownership of the system**

02

Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **Backdoors**, **RootKits**, or **Trojans**

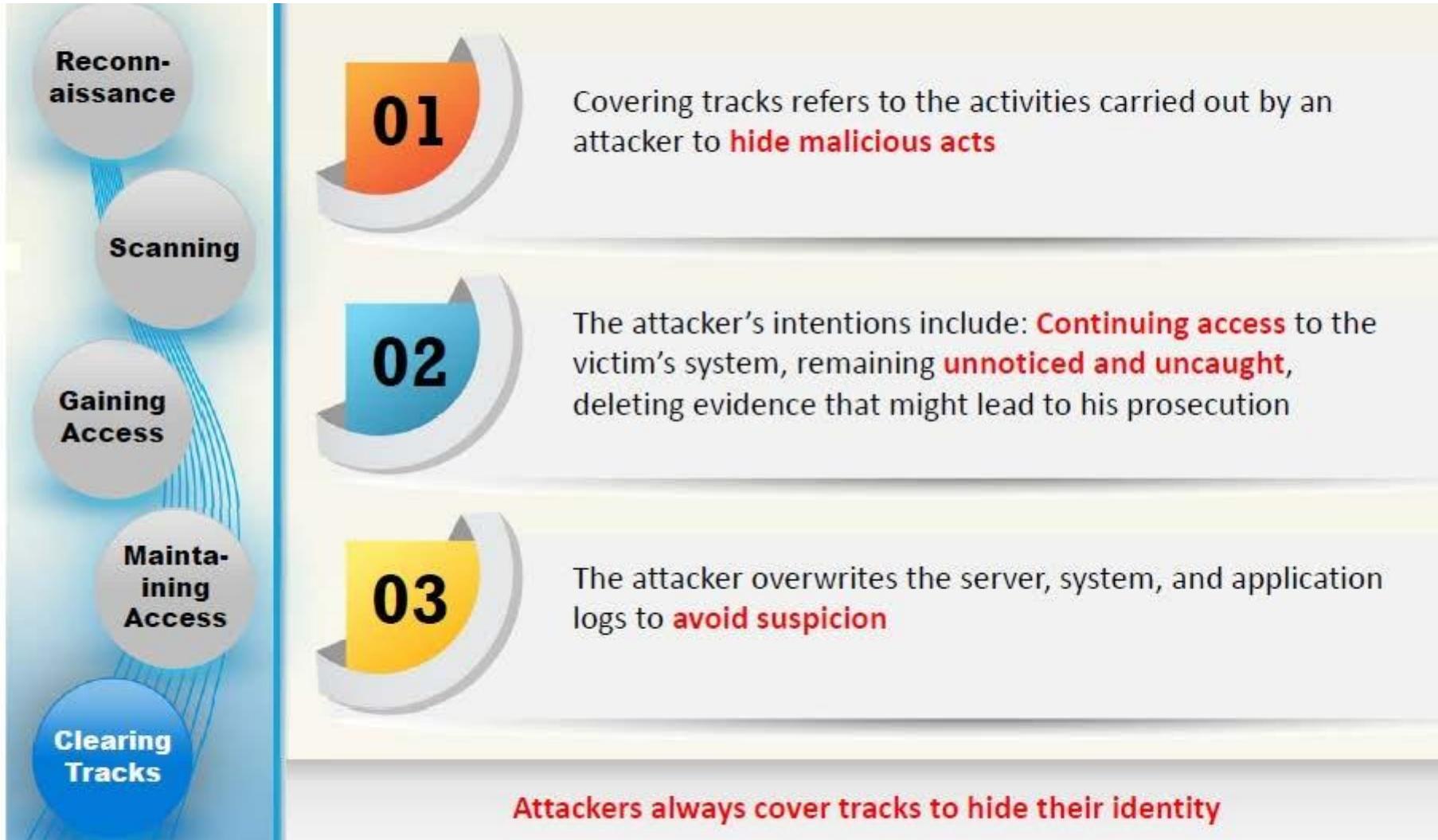
03

Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**

04

Attackers use the compromised system to **launch further attacks**

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