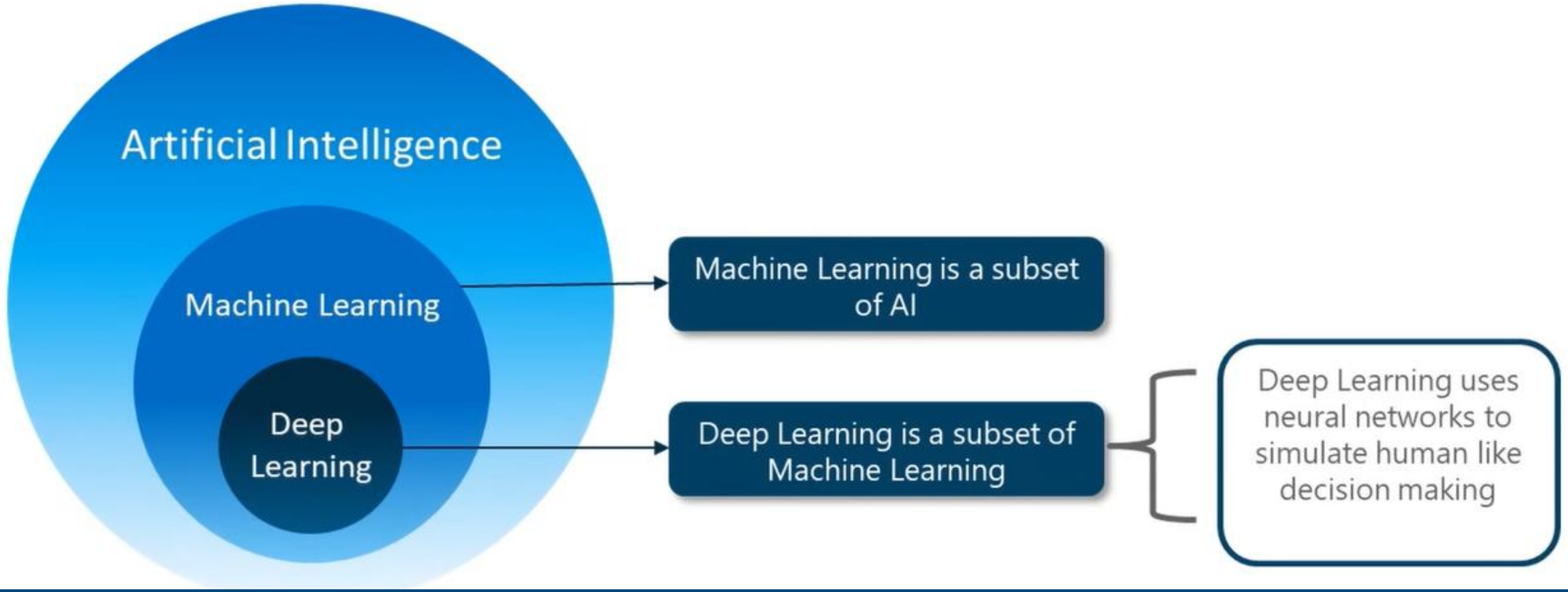
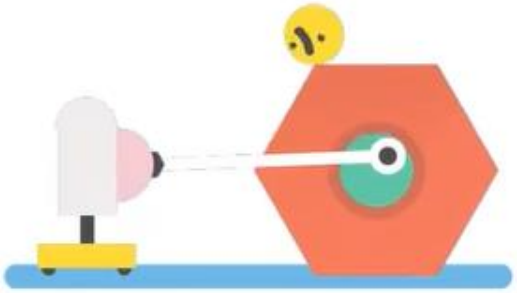
AI vs ML vs DL


Artificial Intelligence
Machine Learning
Deep Learning
Machine Learning is a subset of AI
Deep Learning is a subset of Machine Learning
Deep Learning uses neural networks to simulate human like decision making

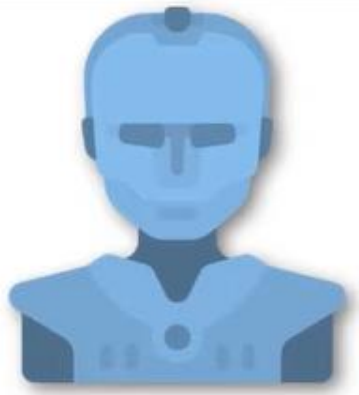
What is Artificial Intelligence?

AI is a technique that enables machines to mimic human behaviour.



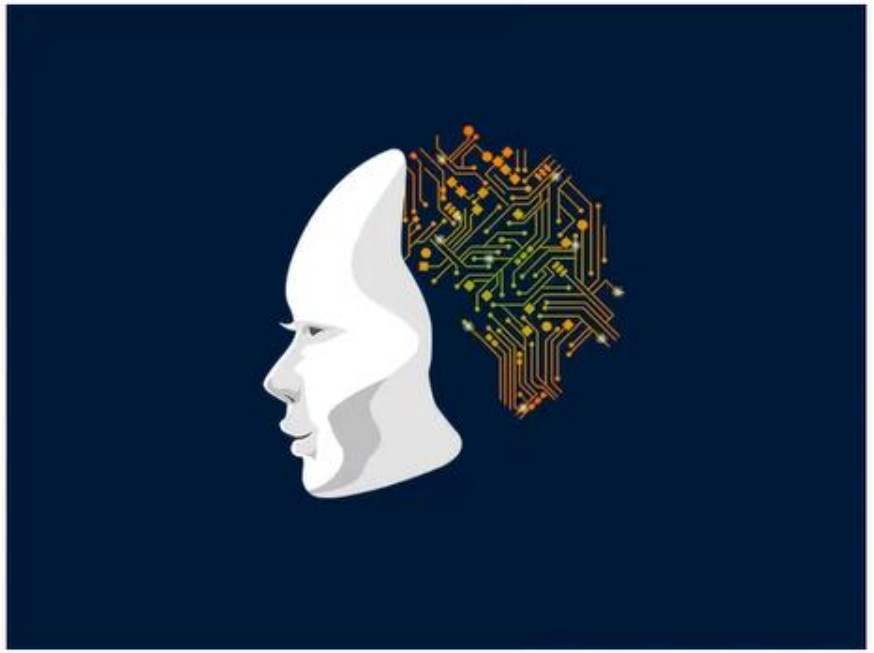
What is Artificial Intelligence?

ARTIFICIAL + INTELLIGENCE = ARTIFICIAL INTELLIGENCE



Artificial intelligence is intelligence exhibited by machines, rather than humans or other animals. The field of AI research defines itself as the study of "intelligent agents": any device that perceives its environment and takes actions that maximize its chance of success at some goal

What is Machine Learning?



Machine learning is the study of computer algorithms that improve automatically through experience. It is seen as a subset of artificial intelligence.

Types of Cyber Attacks

Malware

01

Phishing

02

Password Attacks

03

DDoS

04

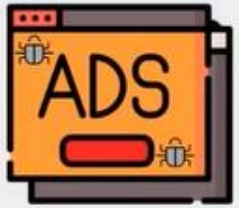
Man in the Middle

05

Drive-By Download

06

Malvertising

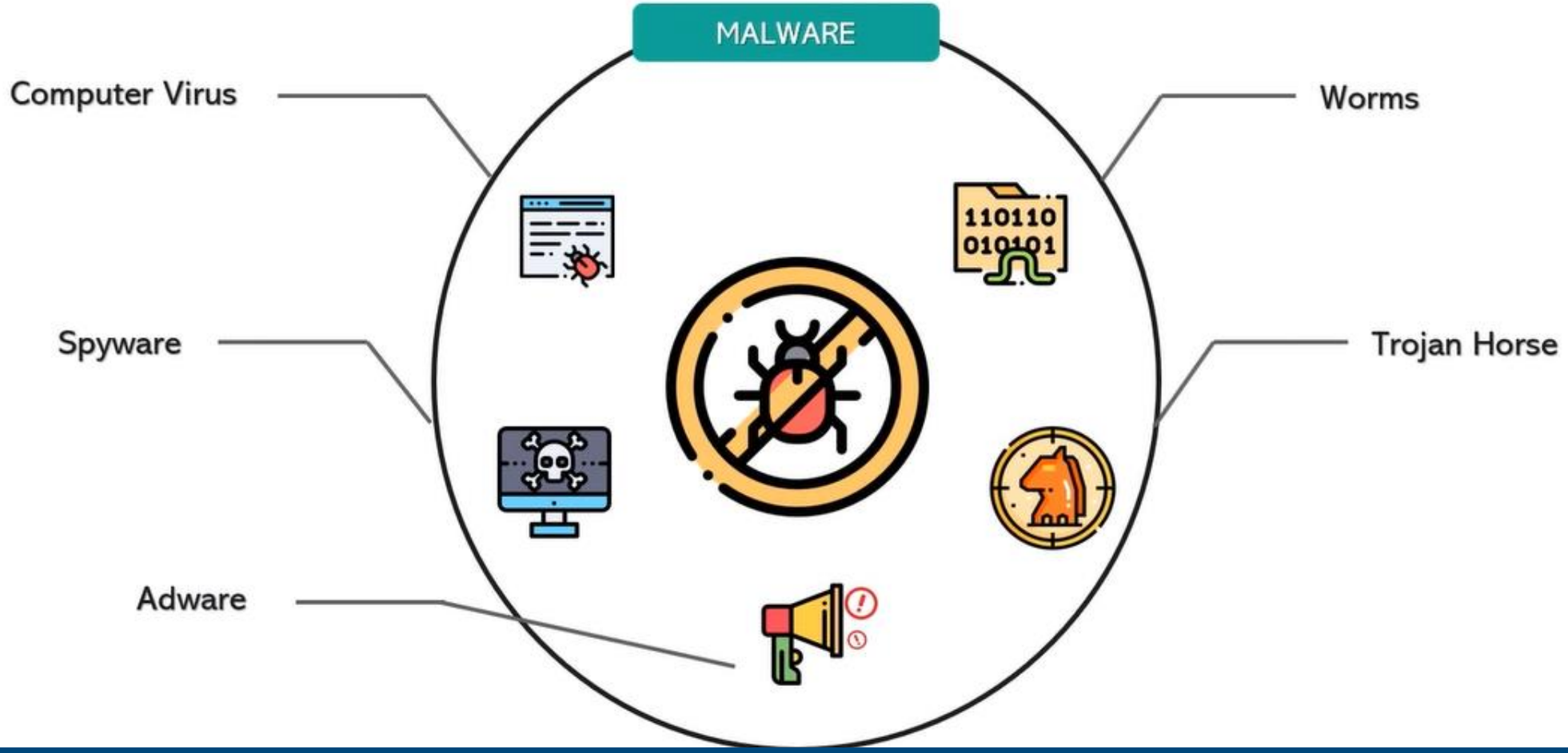


07

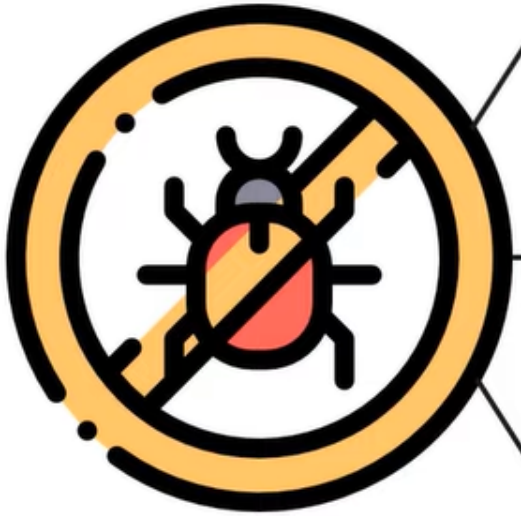
Rogue Software

08

Malware


MALWARE
Computer Virus
Worms
Spyware
Trojan Horse
Adware
110110
010101

How Malware?



Email Attachments

Software Downloads

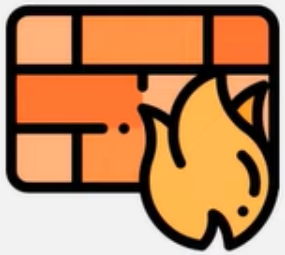
OS Vulnerabilities

Stop Malware

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

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

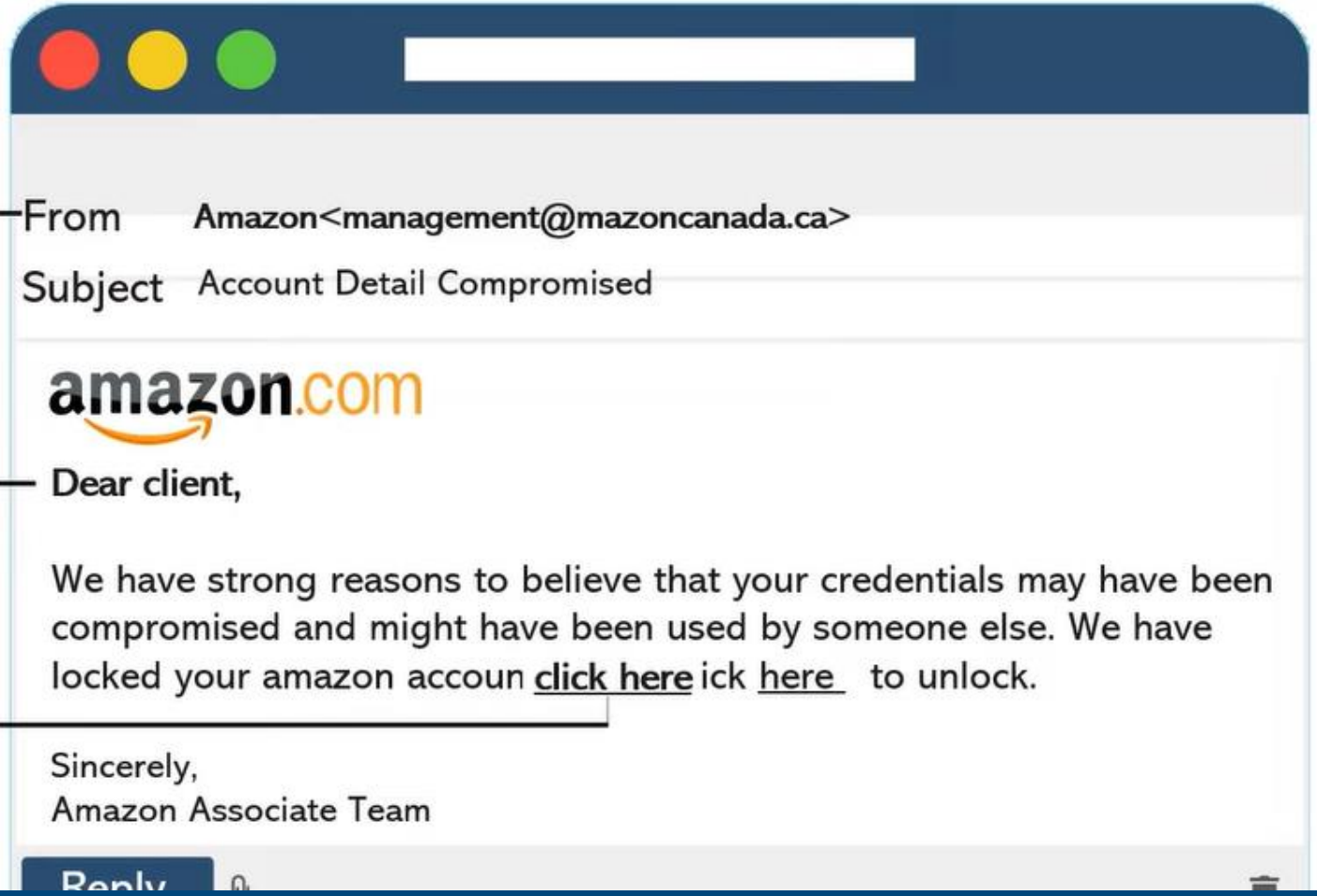
Impersonating

Phishing Awareness

Always check the sender email address

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

Brute Force Attacks

Dictionary Attacks

Keylogger Attacks

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

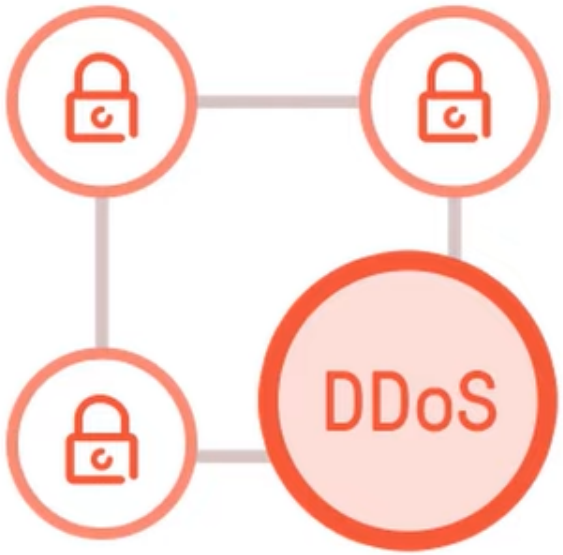
Use Alpha-Numeric

- ✓ 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 Service

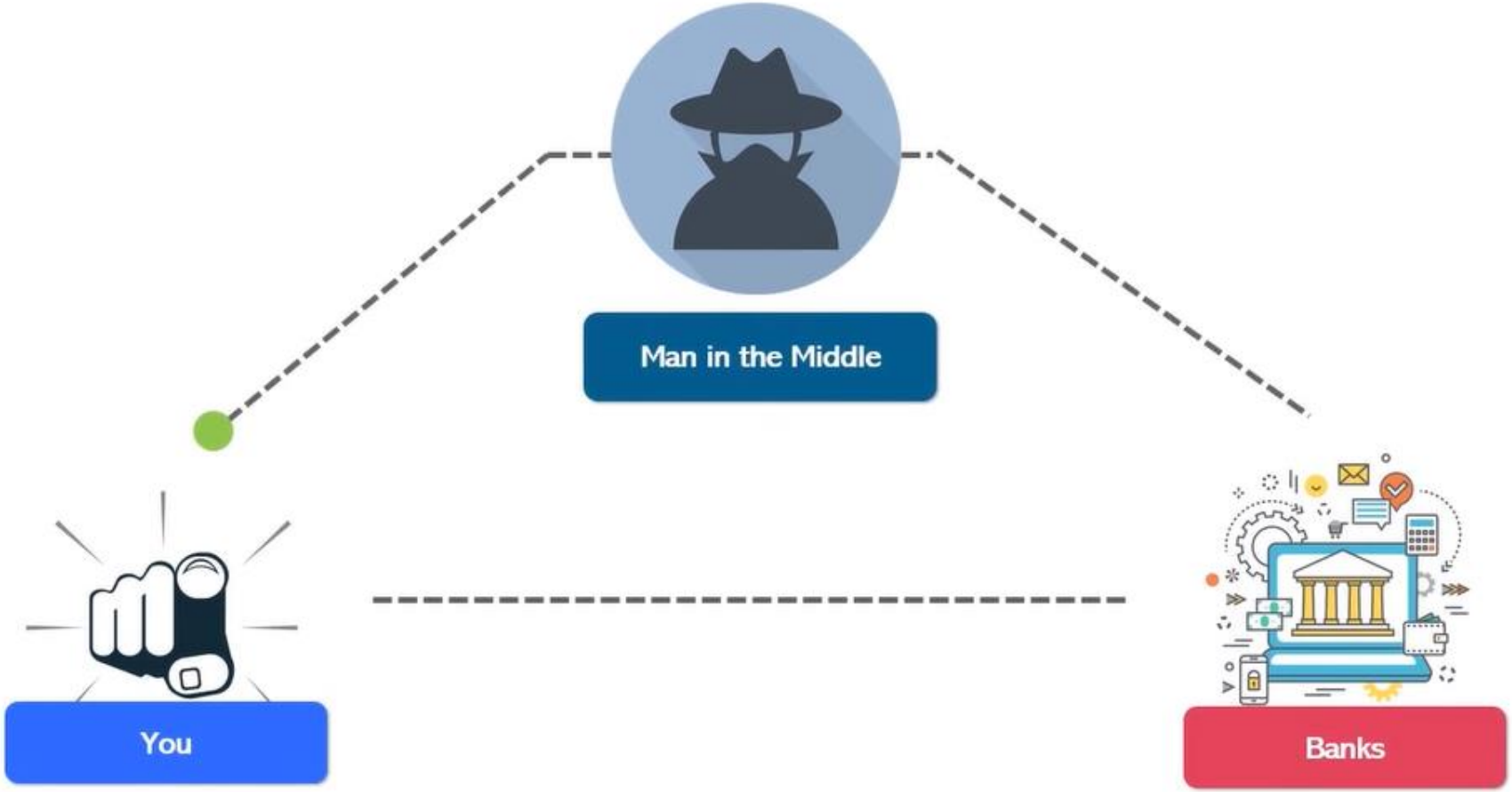


Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.

Prevention

- Traffic Analysis
- Traffic Control
- Recovery Management

Man in the Middle



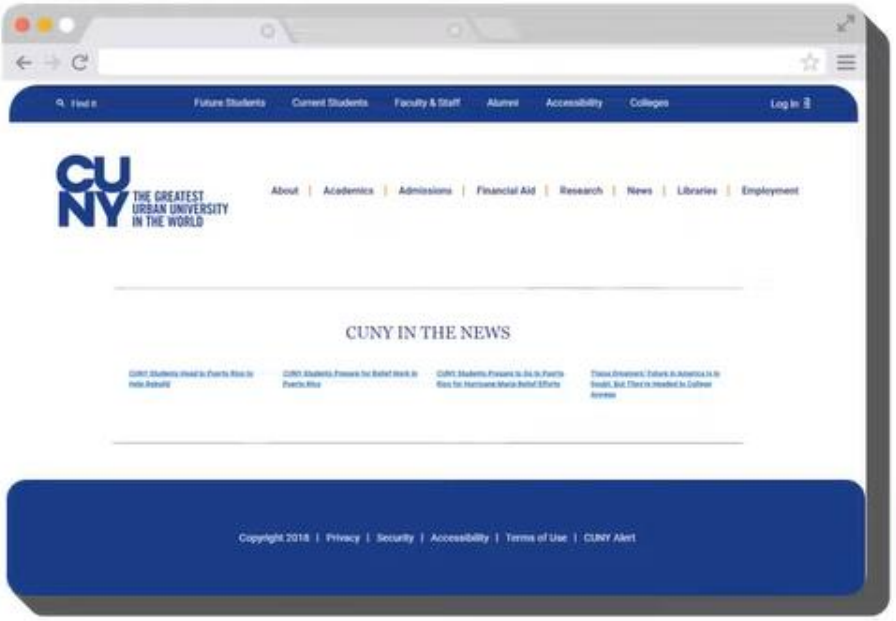
Prevent MITM

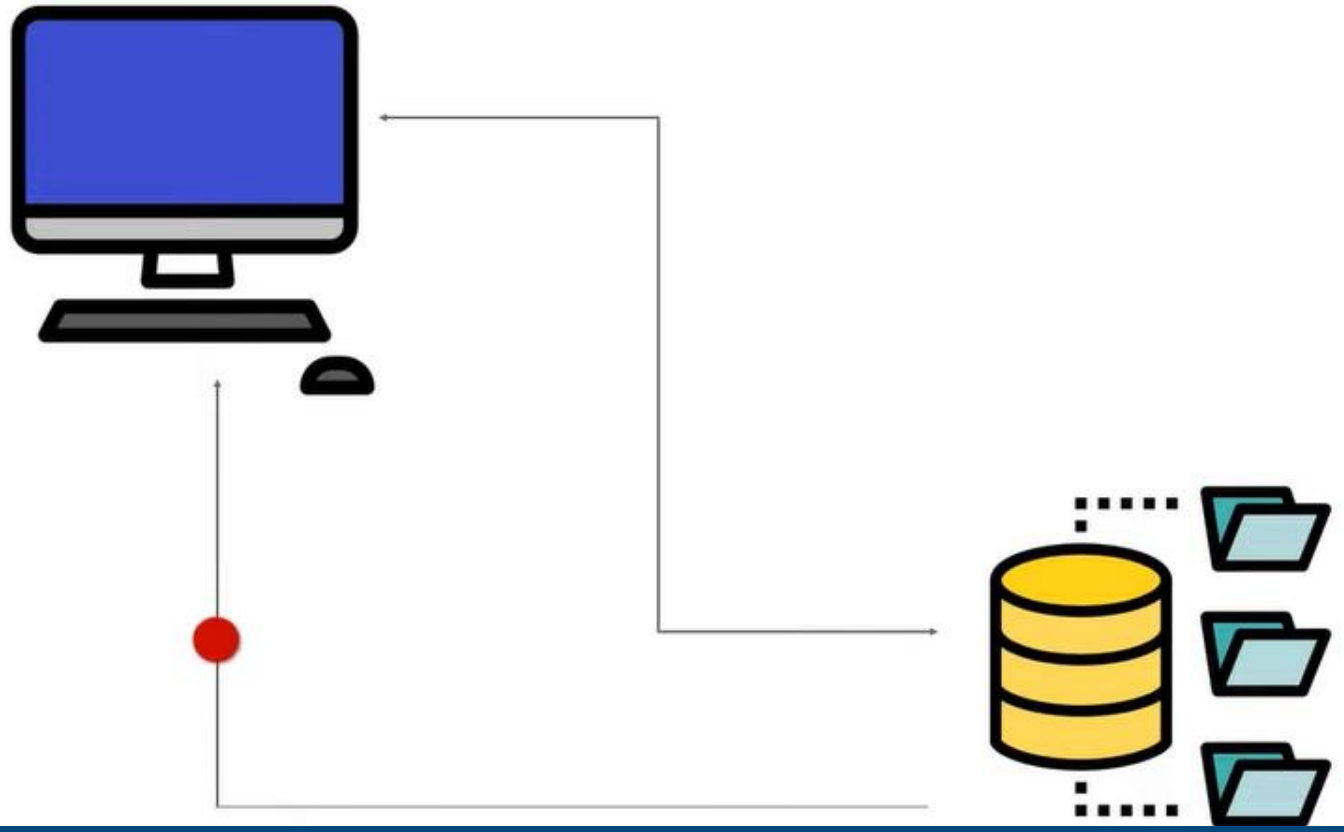
- Use encrypted WAP
- Always check the security of you connection(HSTS/HTTPS)
- Invest in a VPN

What is a 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.

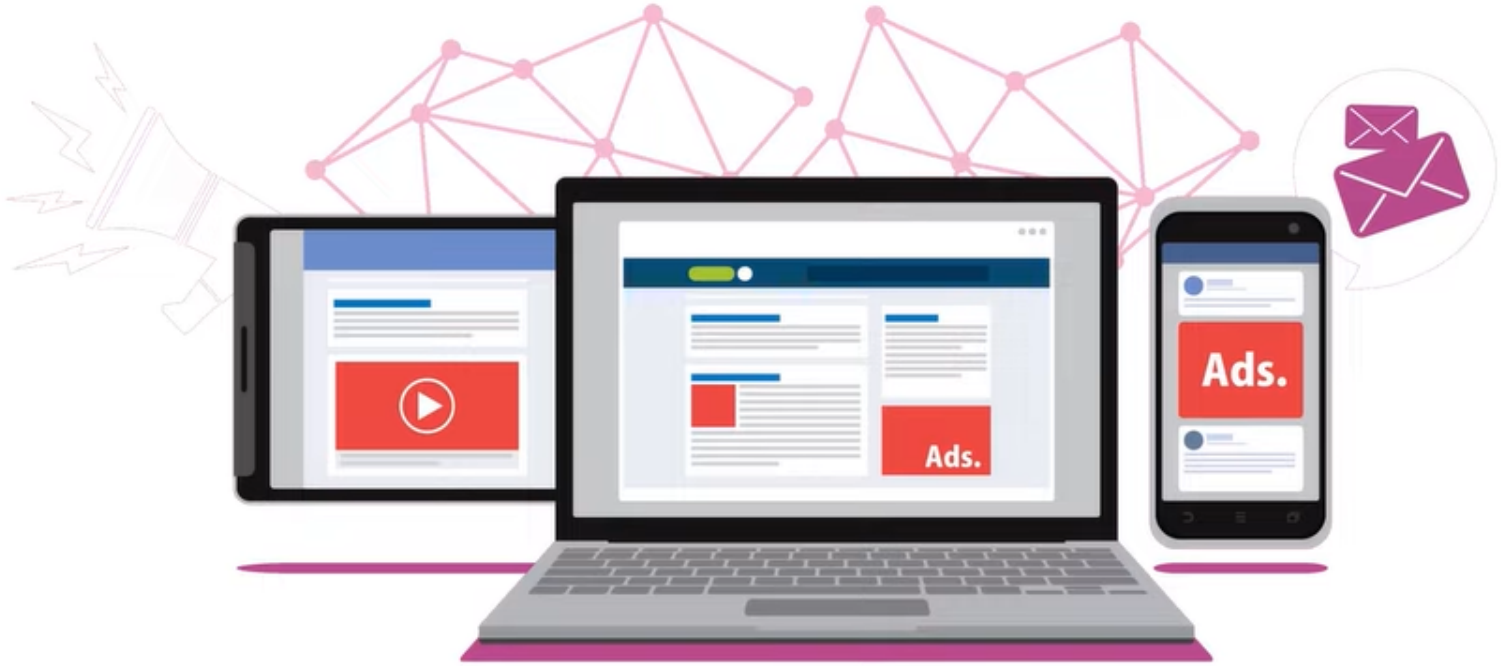
How it works?


Future Students
Current Students
Faculty & Staff
Alumni
Accessibility
Colleges
Log In
CUNY
THE GREATEST URBAN UNIVERSITY IN THE WORLD
About
Academics
Admissions
Financial Aid
Research
News
Libraries
Employment
CUNY IN THE NEWS
Copyright 2018 | Privacy | Security | Accessibility | Terms of Use | CUNY Alert

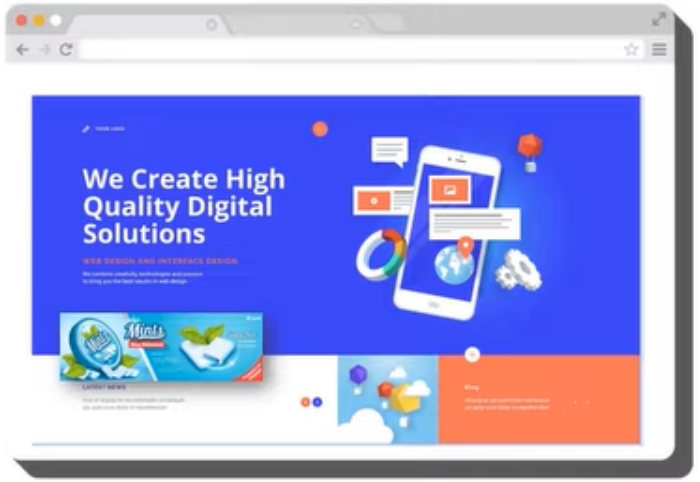


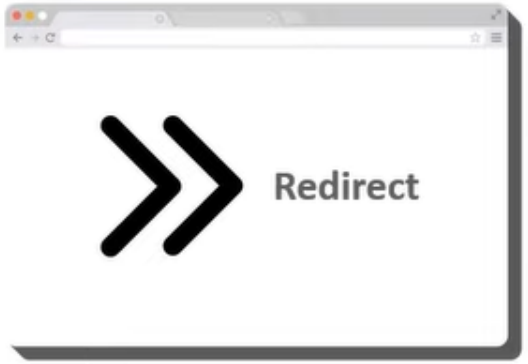
Malvertising

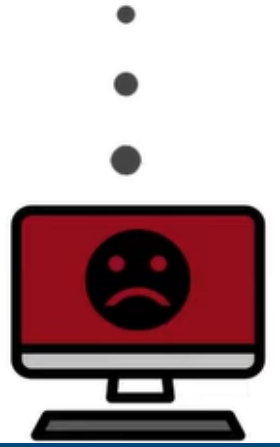
Malvertising is the name we in the security industry give to criminally-controlled adverts which intentionally infect people and businesses.



How does it work?







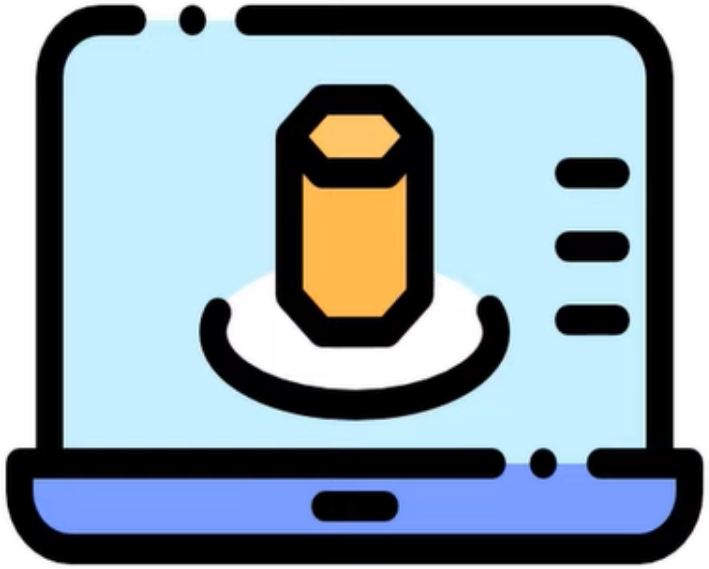
Prevention

Adblocker

Regular Software Updates

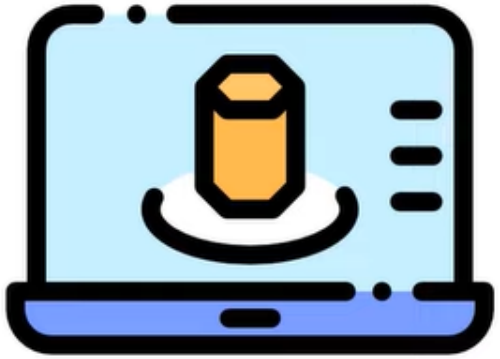
Common Sense

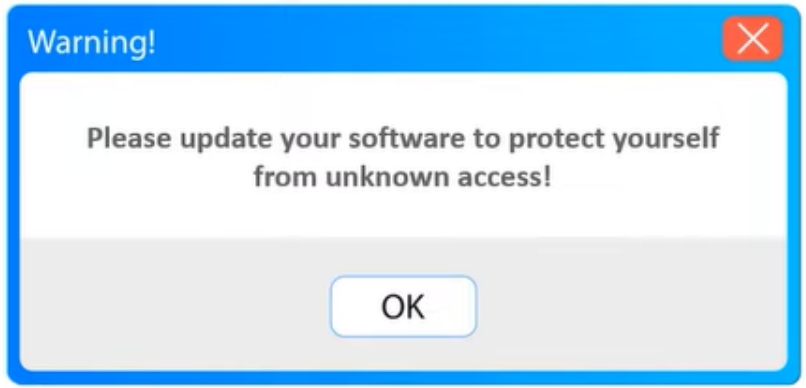
Rogue Software



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.

Propogation



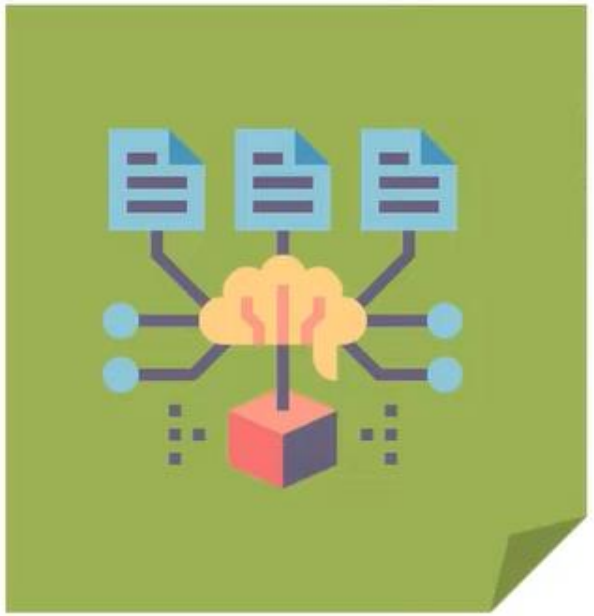


Prevention

Updated Firewall

Use Efficient Antivirus

General Distrust



Behavioural Modelling

AI can be applied to real-time modelling of Net Nodes, Log and audit files an on all Network Traffics

AI/ML in Adaptive Access

Zero Day Attacks

AI modelling can mitigate risks of having new malware that has no define signature

AI/ML in Vulnerability Detection

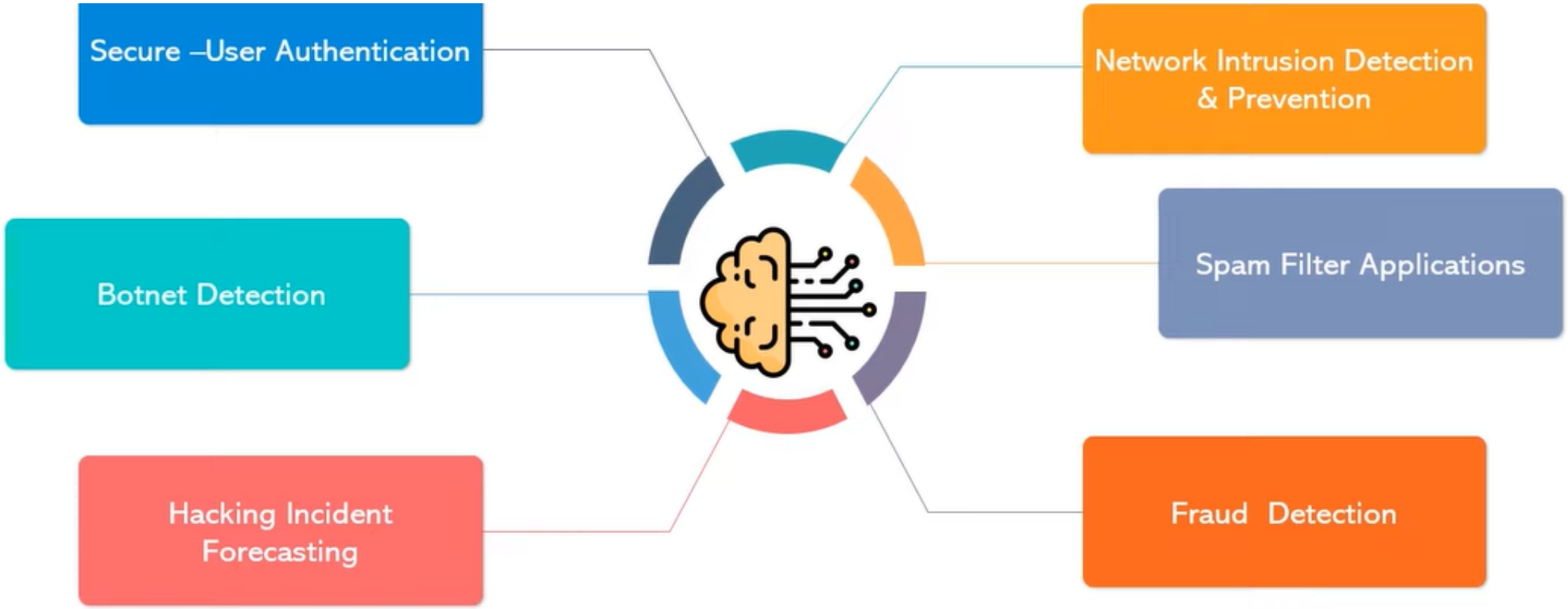
Malware Creation

Smart Botnets

Spear Phishing

Conditional Attacks

Offensive Artificial Intelligence



Applications of Artificial Intelligence in Cybersecurity