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.'
- --

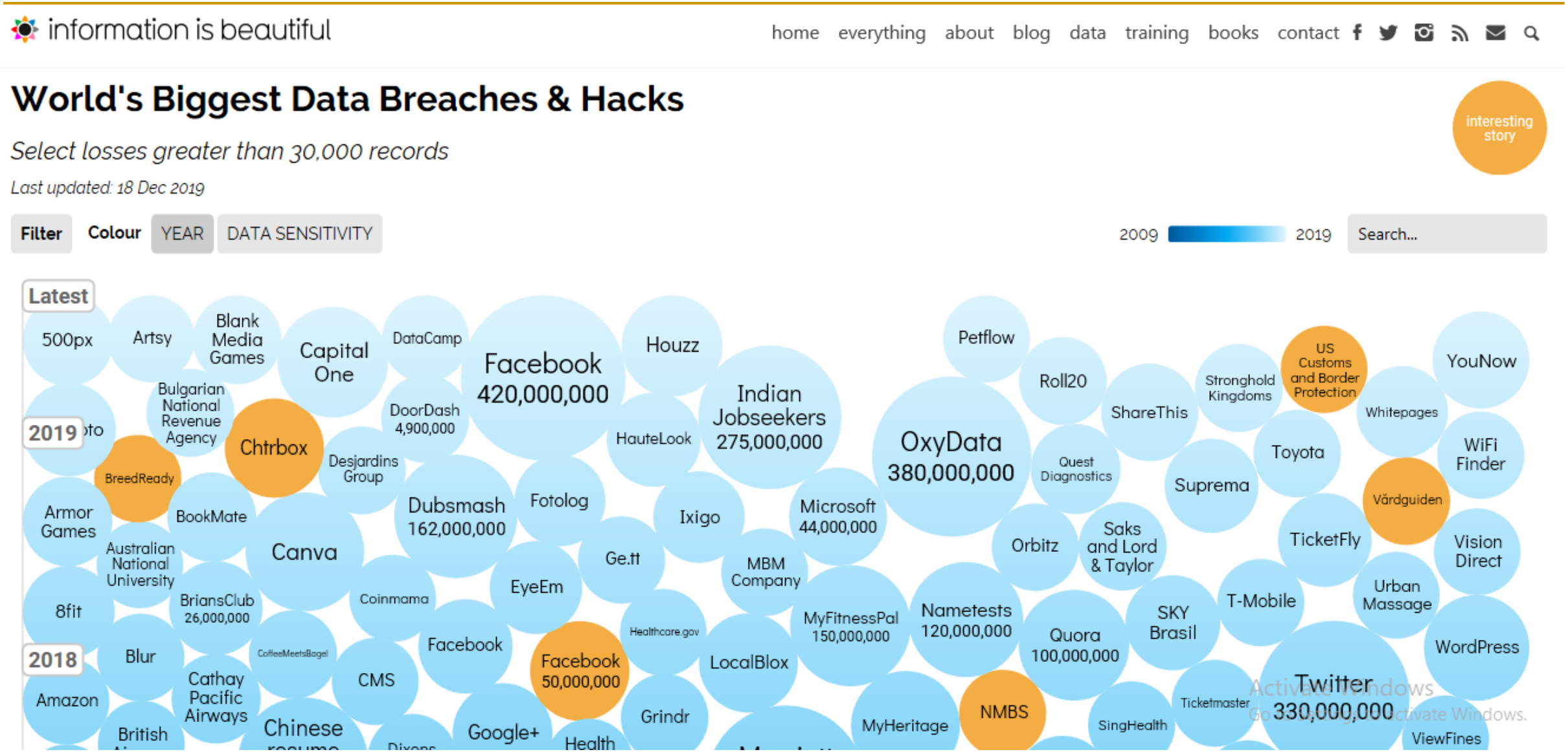
Why We Need Cyber Security???

A Digital Era.

- Computer systems and networks are all around us.
  - Online banking
  - Automated supermarket checkouts
  - Online classes
  - Online shopping
  - Online travel resources

Golden Age for Data Exploits

History of Cyber Attacks



Cyber Security?

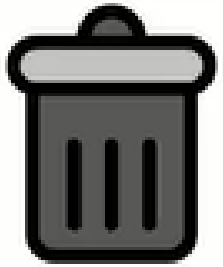
Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.

Cyber Security?

- **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?

Unauthorised Modification



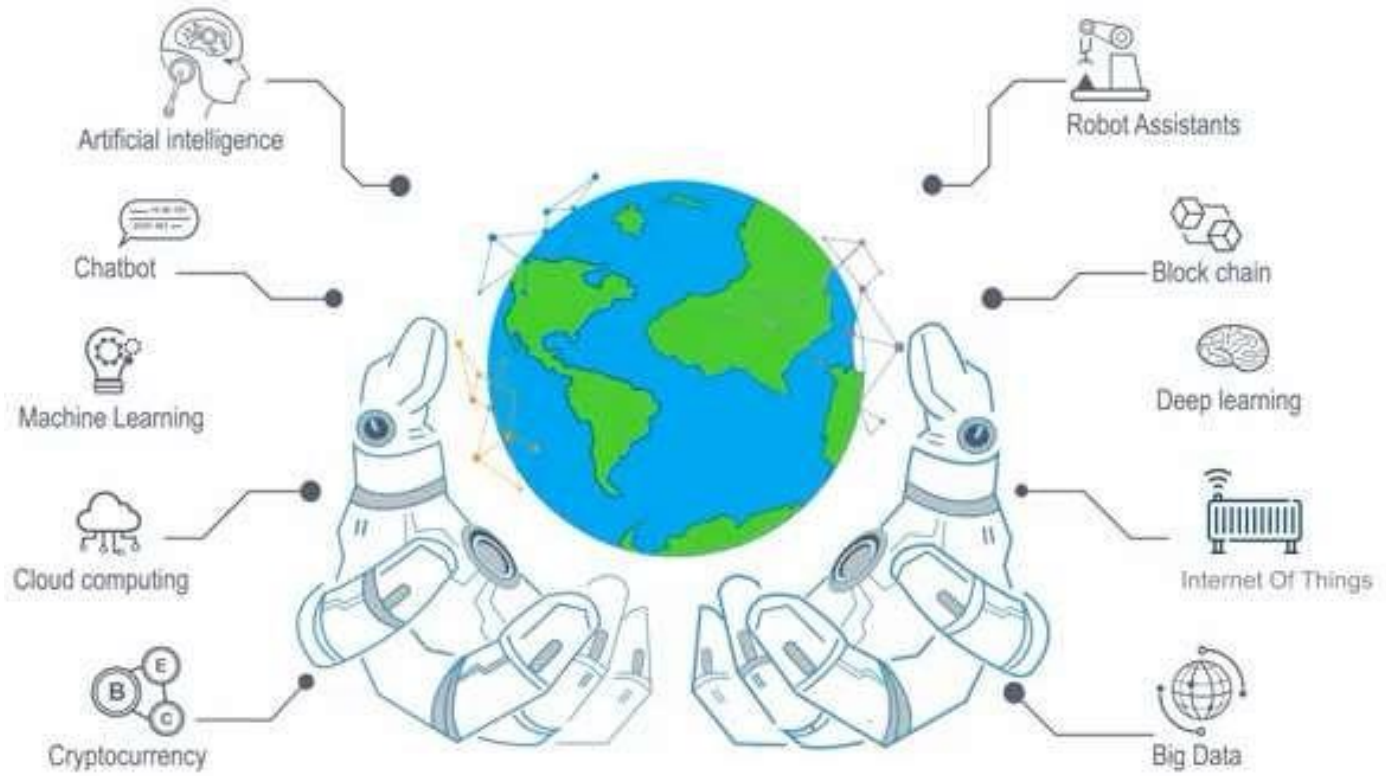
Unauthorised Deletion

Unauthorised Access

Top 10 Reasons to Learn Cybersecurity


10

10. Evergreen Industry



9. The World is Your Oyster

Highly transferable skills mean you can move anywhere in the world

Top countries you could travel to:

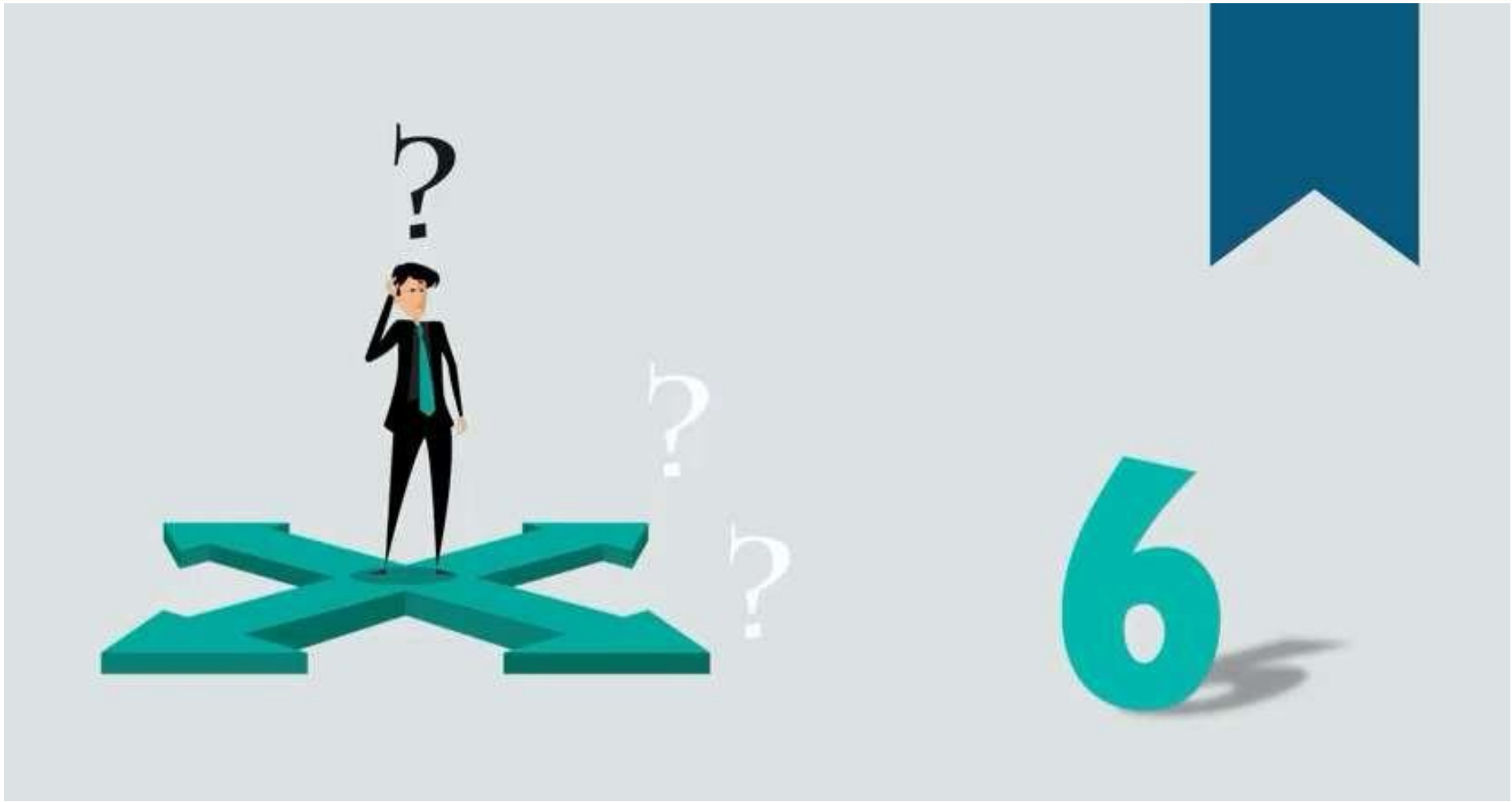
- United States of America
- United Kingdom
- Japan
- Russia

8. Working for the Greater Good

As a rule, cybersecurity professionals are not likely to be famous. On the contrary, they quietly provide committed, faithful and honourable service to their organizations, countries and society as a whole.

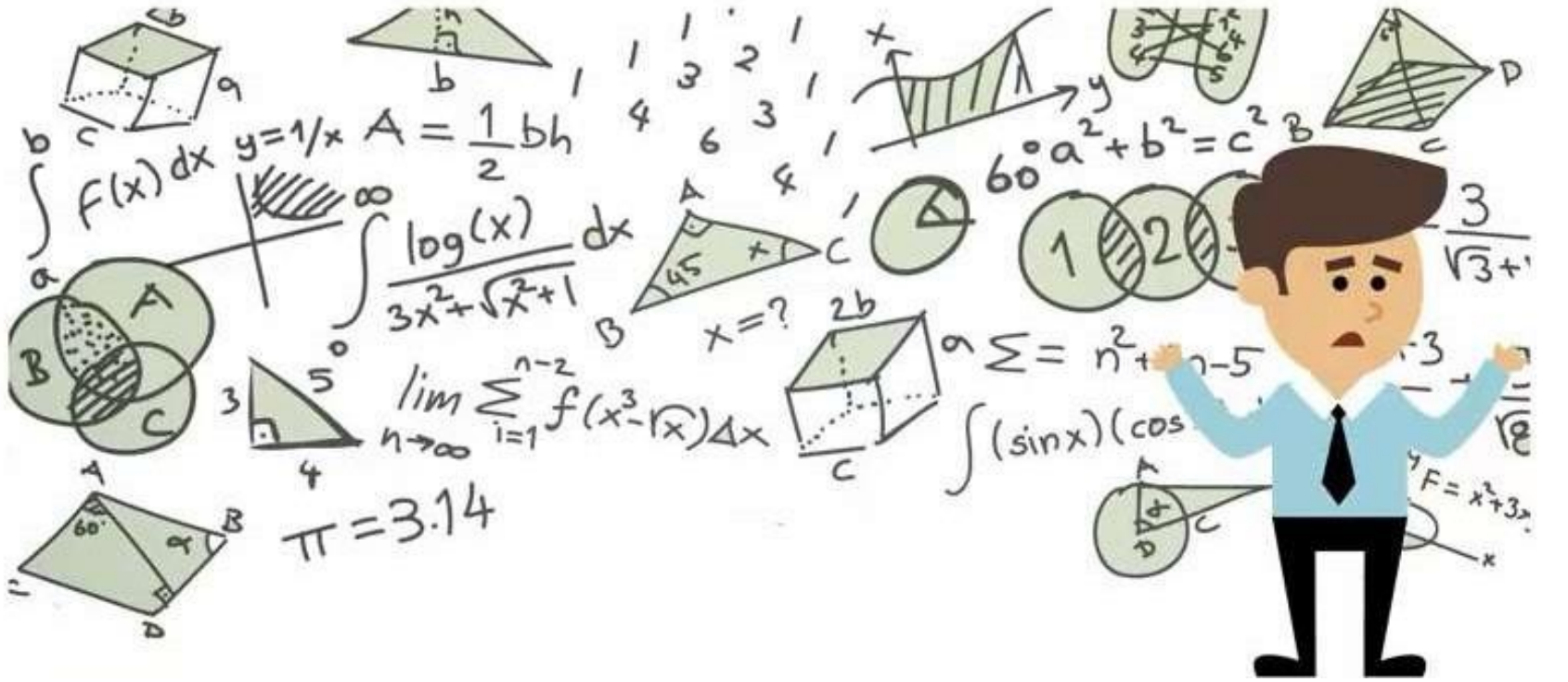
7. Work with Top Secret Agencies

1
1

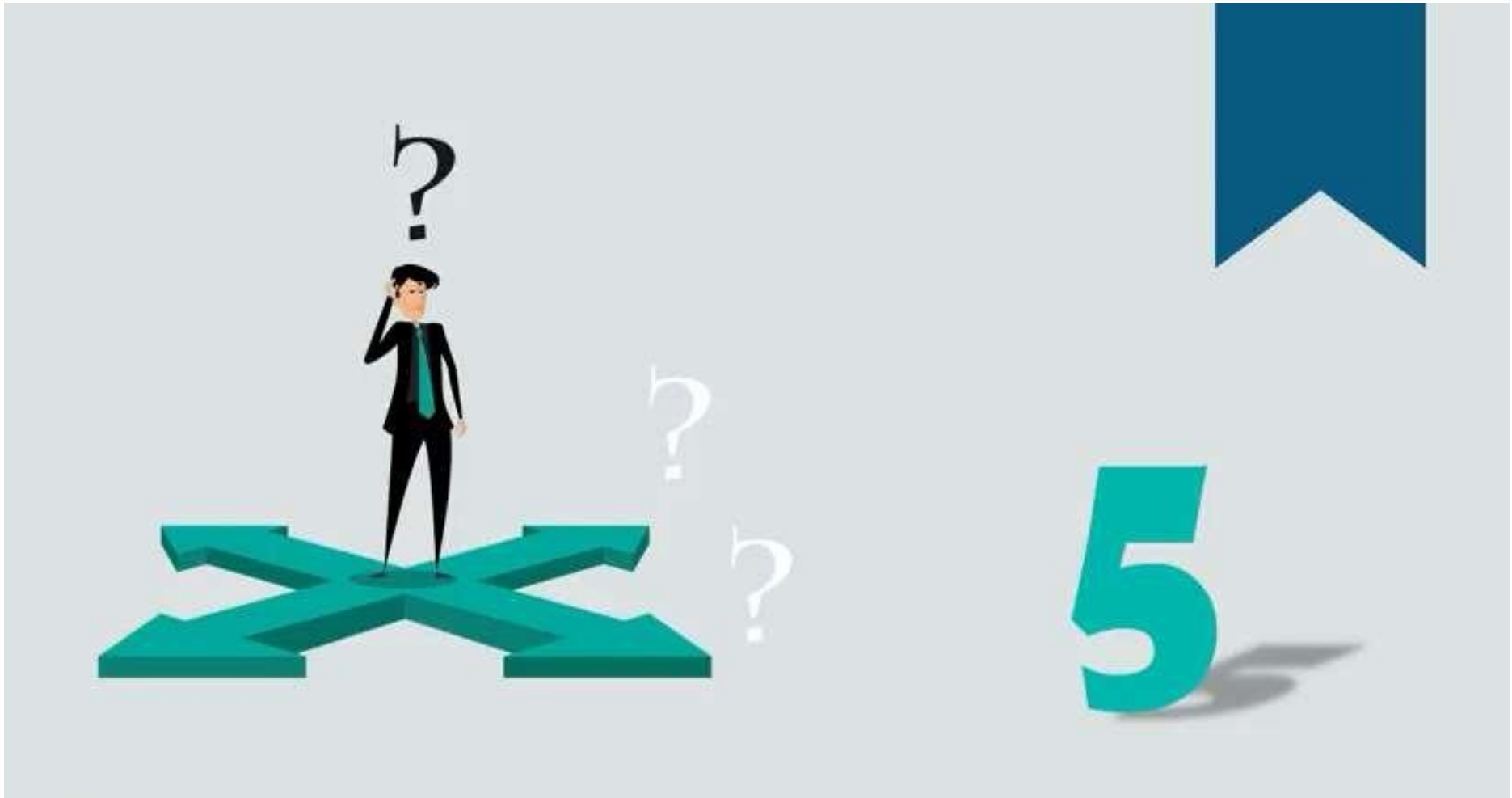


1
2

6. No Concern for Math

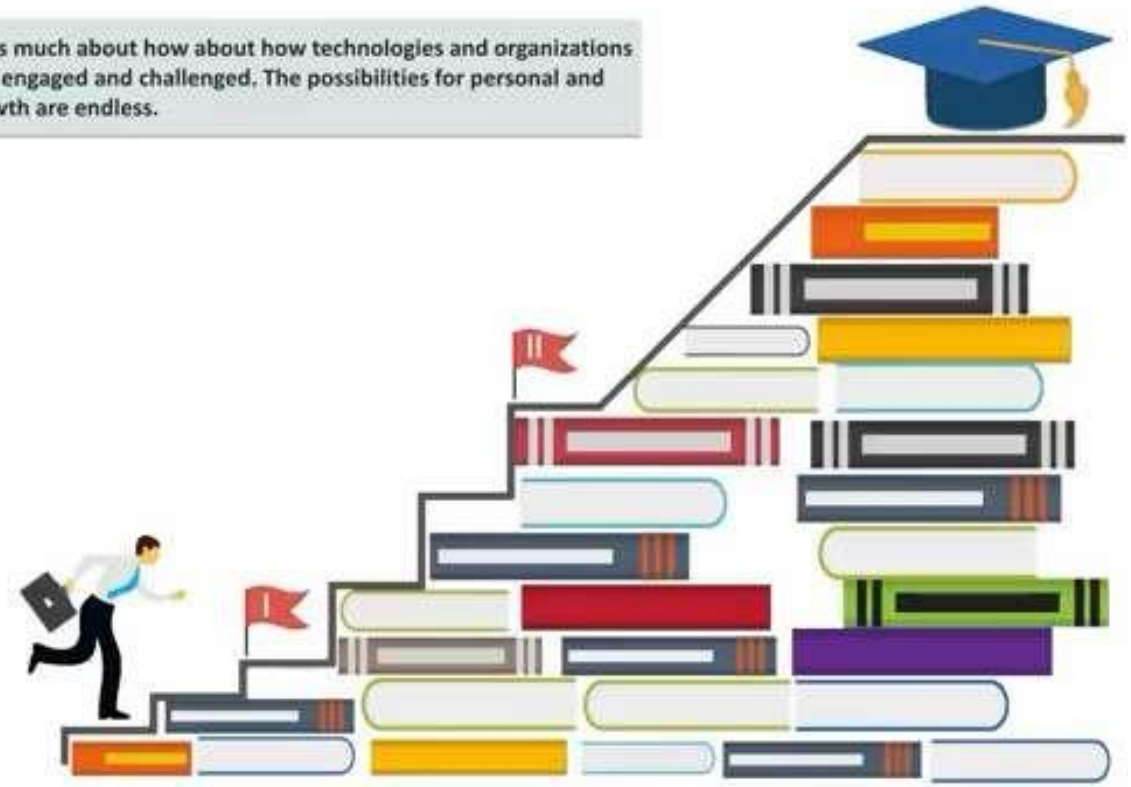


6. No Concern for Math


?
?
?
5

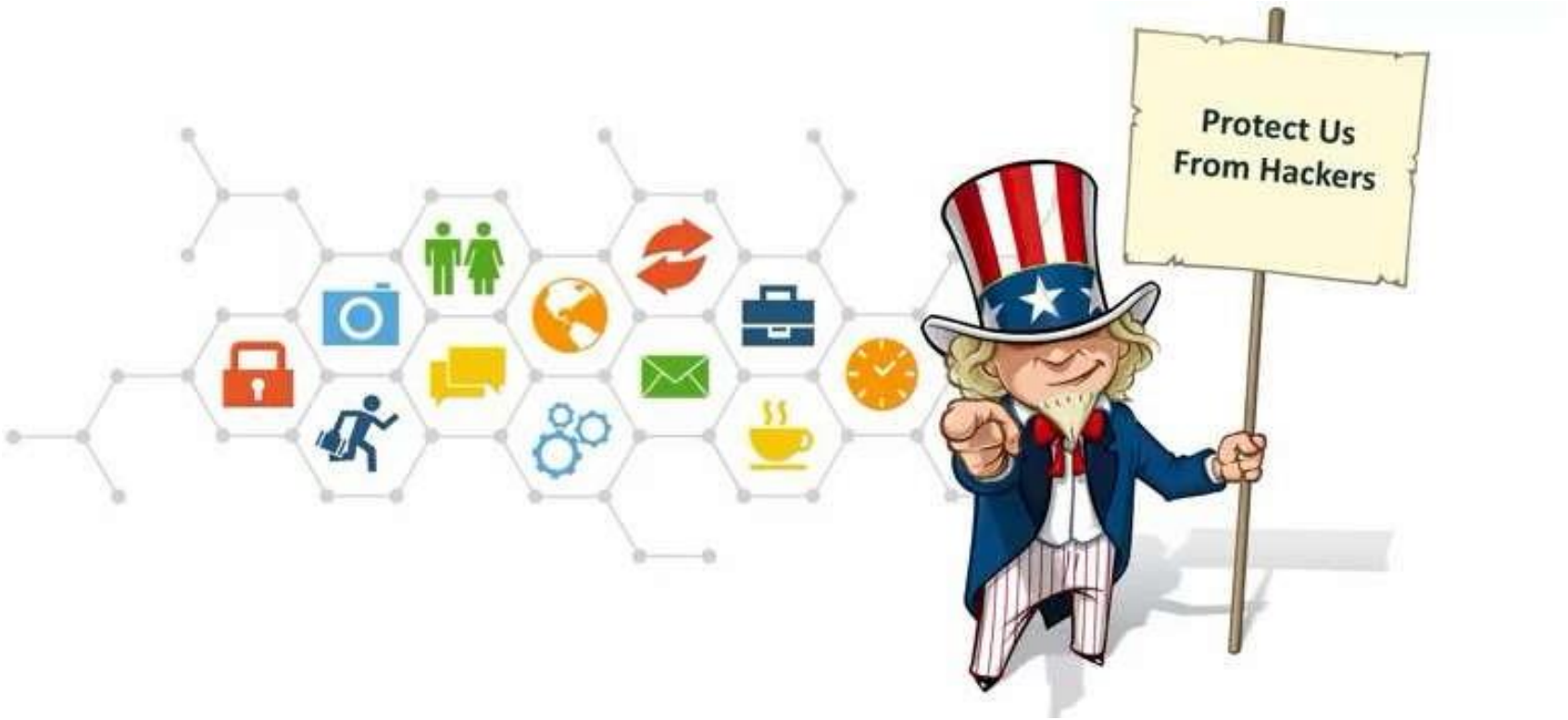
5. Unlimited Growth Potential

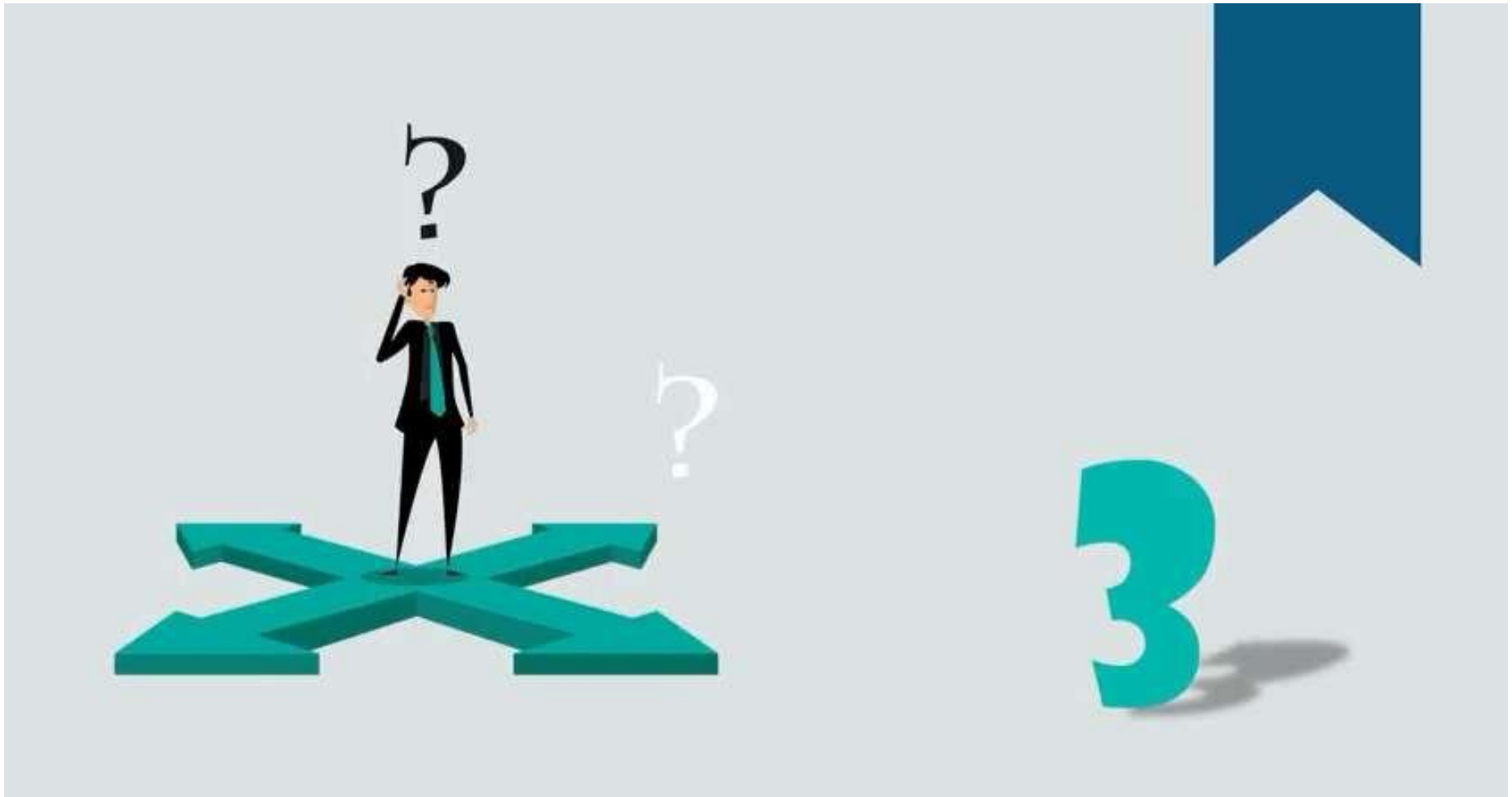
A good cybersecurity professional works to understand as much about how about how technologies and organizations work as possible. That's a massive opportunity to stay engaged and challenged. The possibilities for personal and career growth are endless.




?
?
4

4. Everyone Wants You!




?
?
3

3. Variety of Industries

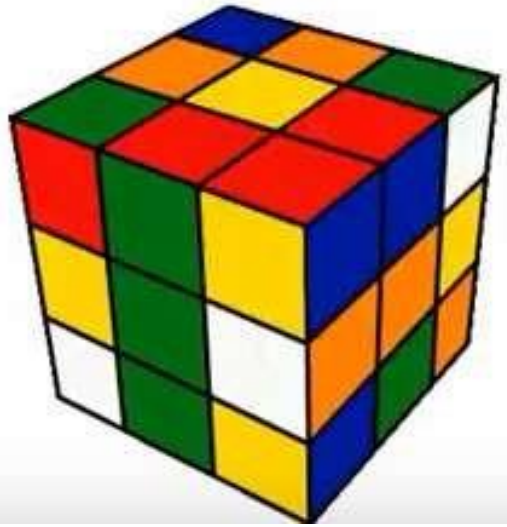
Every industry is going through some sort of digitalisation. And where ever digitalisation occurs, cyber attacks are bound to happens, hence cybersecurity professionals find jobs everywhere.


?
?
2

2. Dynamic and Challenging Jobs

All of the opportunities for growth stem from the variety of technologies and situations security professionals face. If it uses ones and zeros, it has a cybersecurity component, and some roles even extend to physical security!

- Never Gets Boring
- New and Interesting Problems
- Creativity is encouraged



2
2

1. Money Makes the World Go Round

Faced with online attacks, business and government are looking for experts who can protect their systems from cyber criminals – and they are willing to pay high salaries and provide training and development

- Fastest Growing Salaries
- For Seniors, it surpasses the median
- Earning based only on merit

CIA TRIAD (Video)

https://www.youtube.com/watch?v=rwigKjEsdTc

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

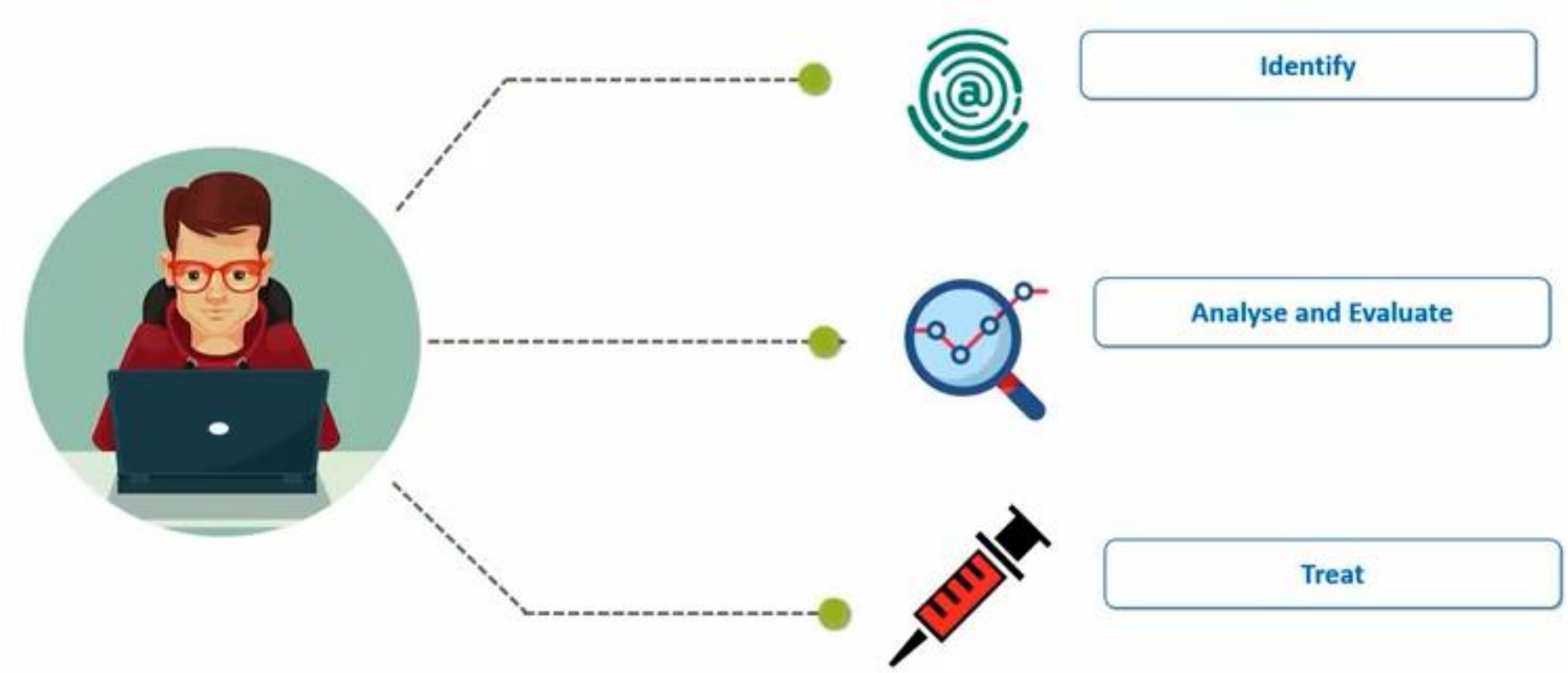
Integrity

- 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

Steps to Fix a Crime



Vulnerability, Threat & Risk

Vulnerability

- Vulnerability refers to the weakness of an asset that can be exploited by one or more attacker
- In context of cyber world, vulnerability refers to a bug/ defect in hardware or software which remains to be fixed and is prone to be exploited to cause a damage to one of the elements within CIA triad

Threat

- A threat is any event that has the potential to bring harm to an organisation or individual
- Natural Threats, Intentional Threats, Unintentional threats
- Threat assessment techniques are used for understanding threats.

Risk

- Risk refers to the potential for loss or damage when a threat exploits a vulnerability
- Risk = Threat x Vulnerability
- Risk management is key to cybersecurity

- How is personal information safeguarded?
- What are the vulnerabilities?
- What secures these systems?

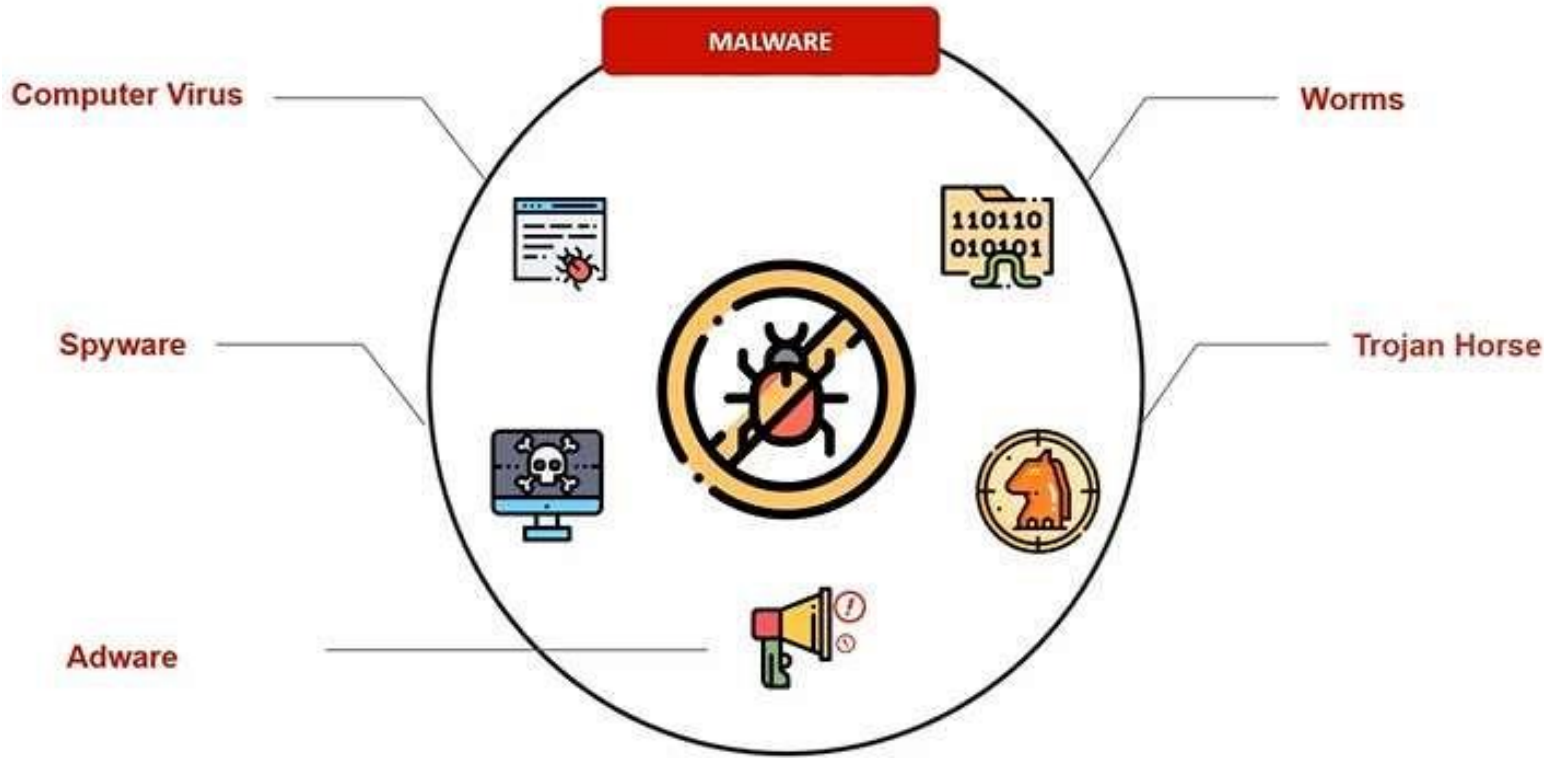
How Seriously Should You Take Threats to Network Security?

- Which group do you belong to?
  - “No one is coming after my computer.”
  - “The sky is falling!”
  - Middle ground.

Cyber Attacks

Types of Attacks

Malware


MALWARE
Computer Virus
Worms
Spyware
Trojan Horse
Adware
110110
010101

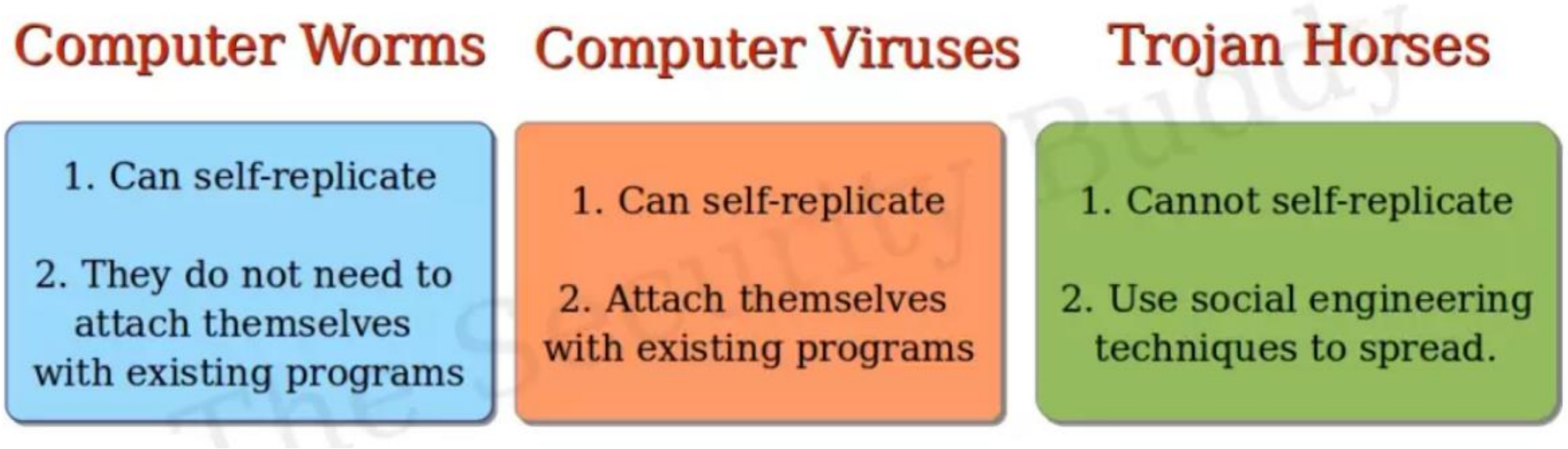
Malware attack

Downloaded

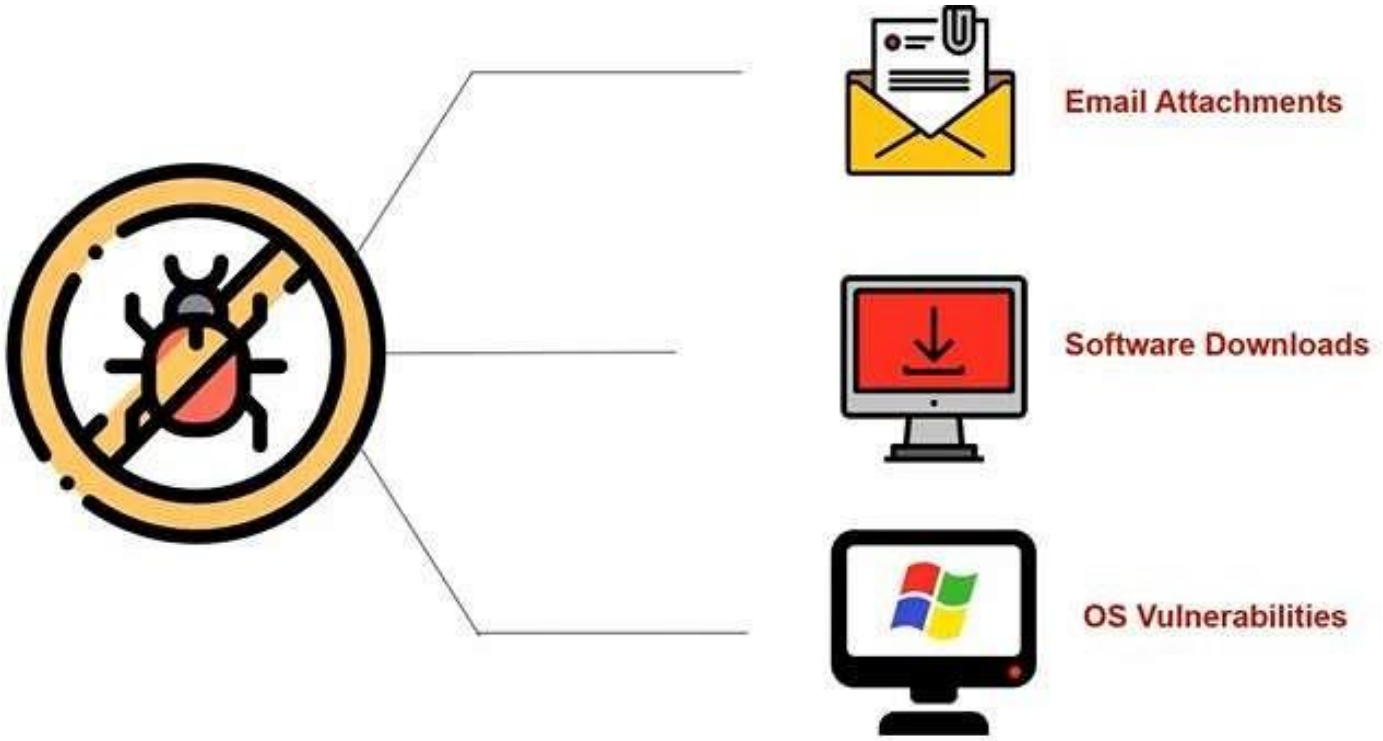
Malware

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.

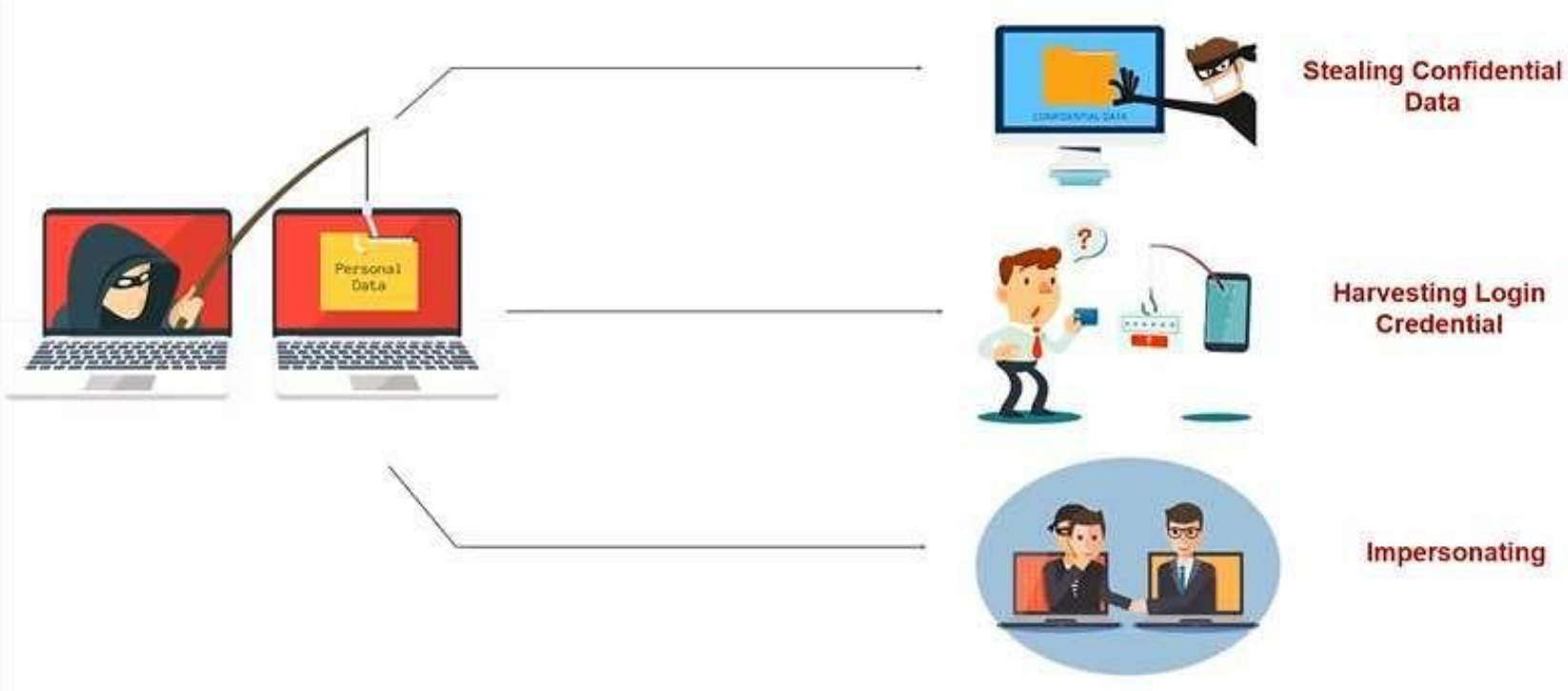
Updated OS

- 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.

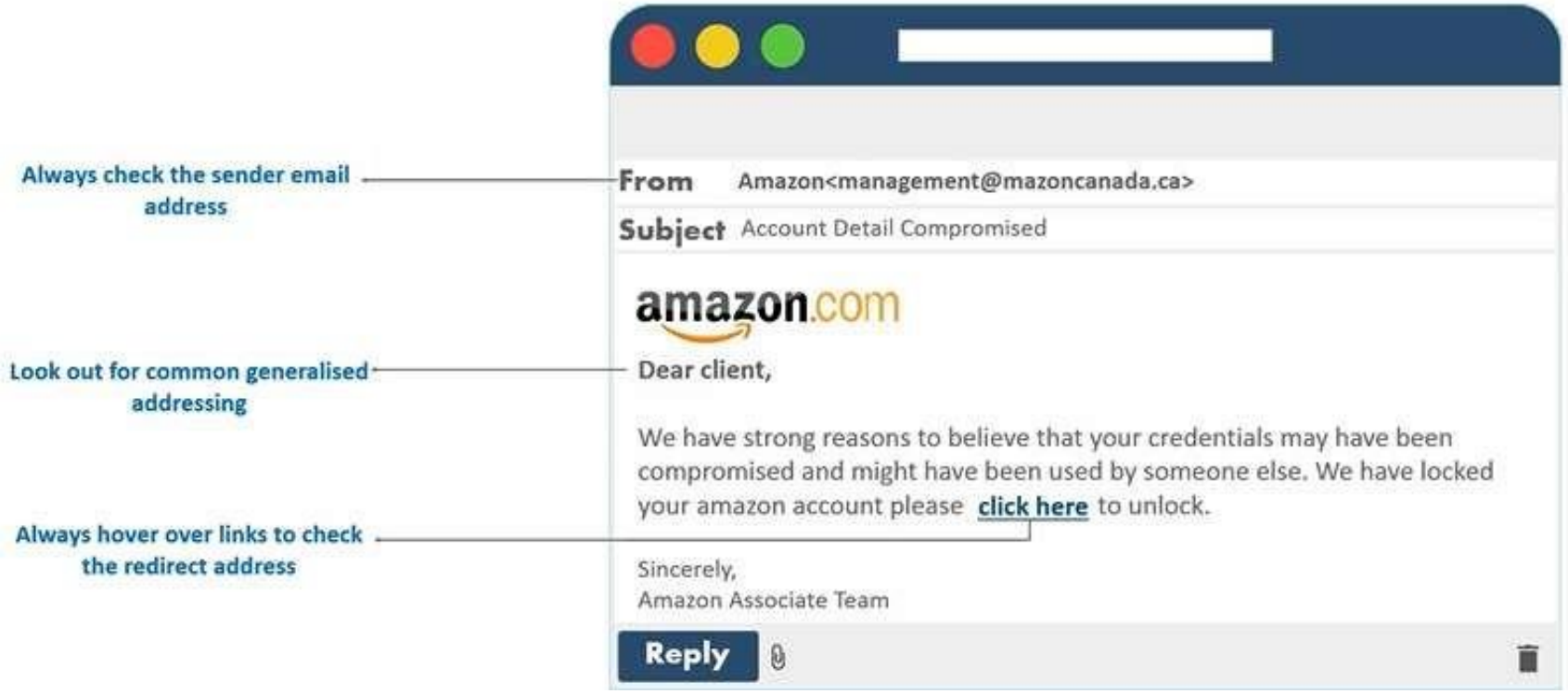
Phishing Attack

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?



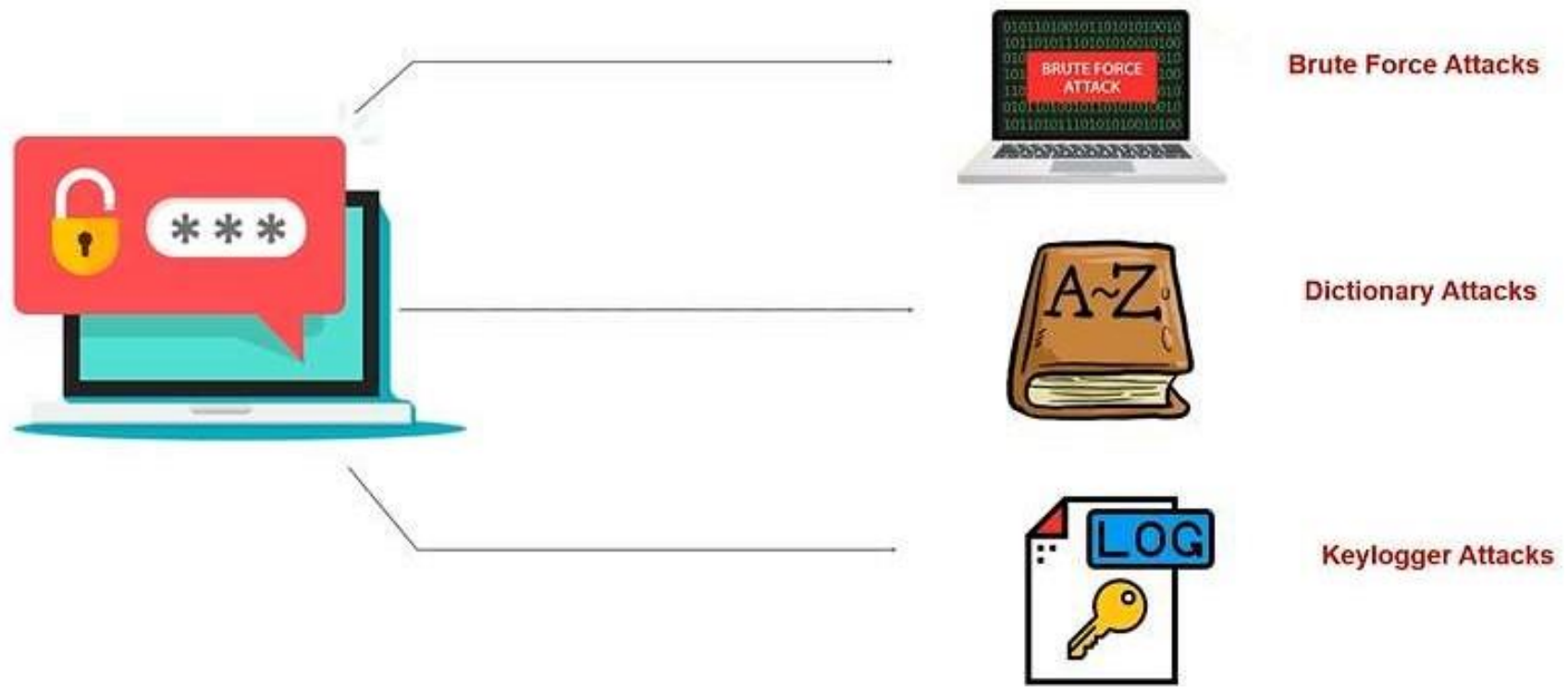
Phishing Awareness



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

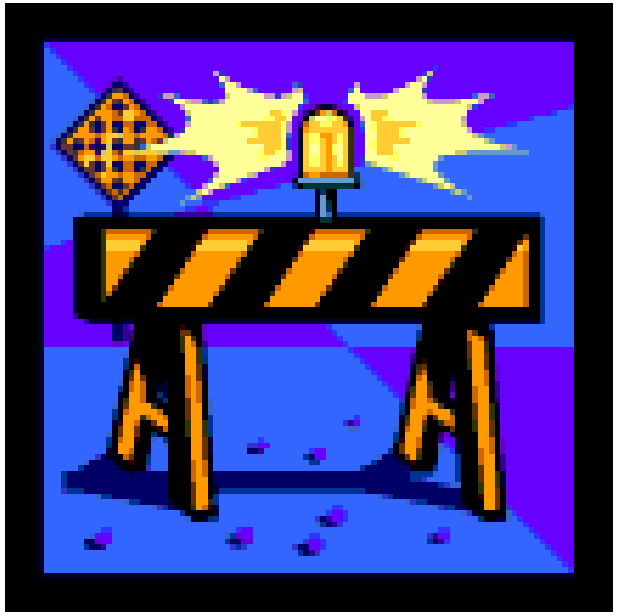
- It's always a great idea to use a password that only makes sense to you
- Passwords which use actual words that make sense are much more susceptible to dictionary attacks

Distributed Denial of Services (DDoS)

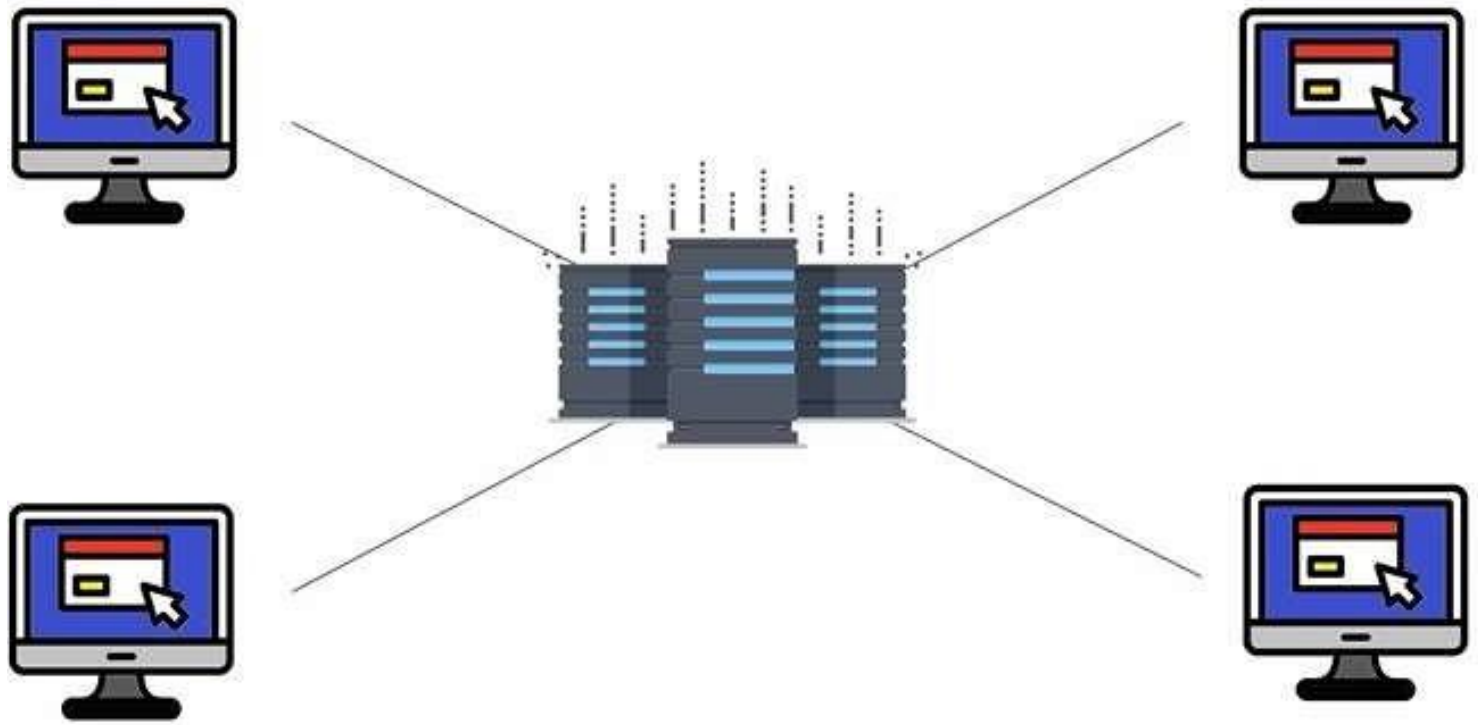
Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.

Denial of Service Attacks

- The attacker does not intrude into the system but just blocks access by authorized users.



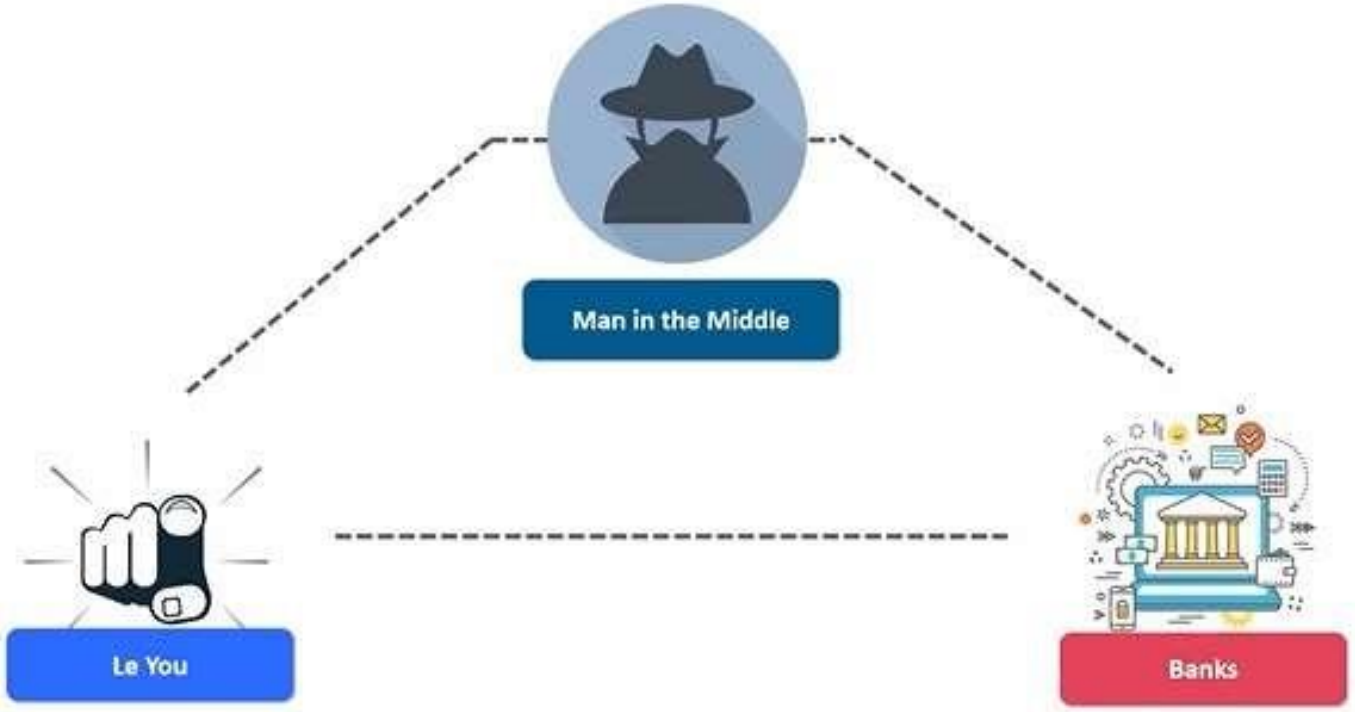
Packet Flood



Prevention

- Traffic Analysis
- Traffic Control
- Recovery Management

Man in the Middle



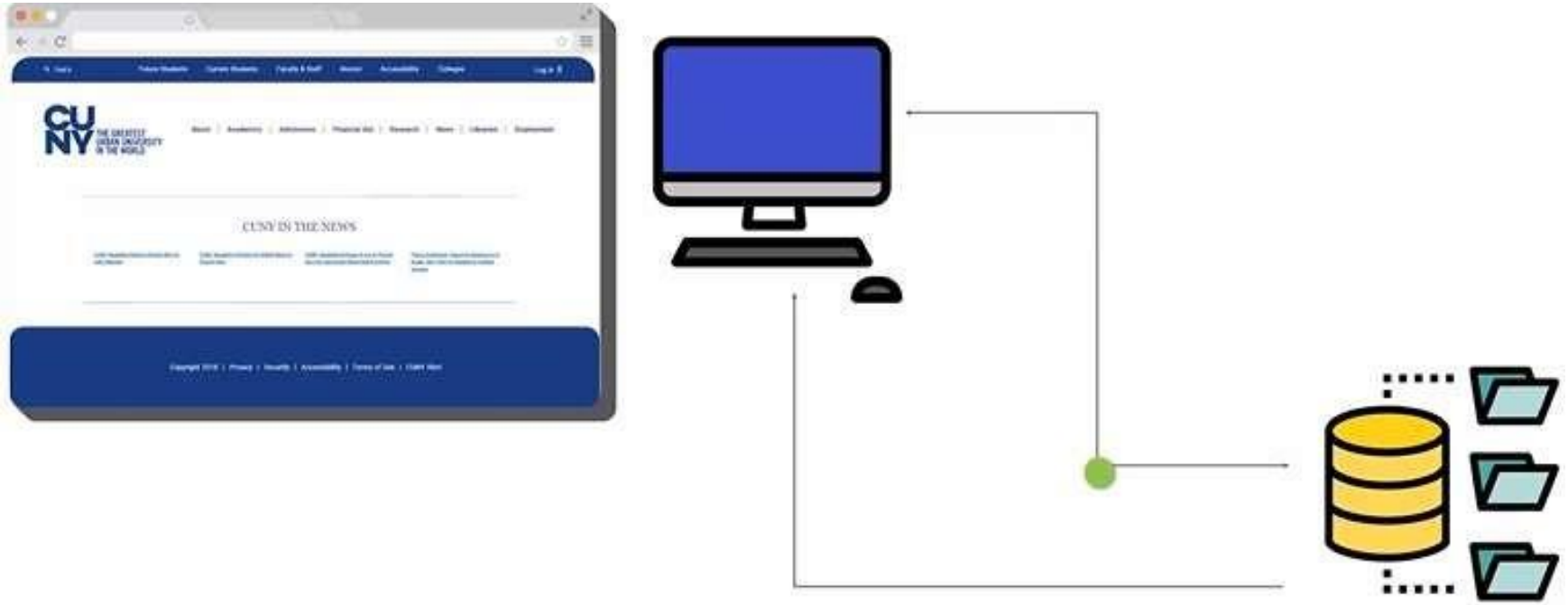
Prevent MITM

- 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.

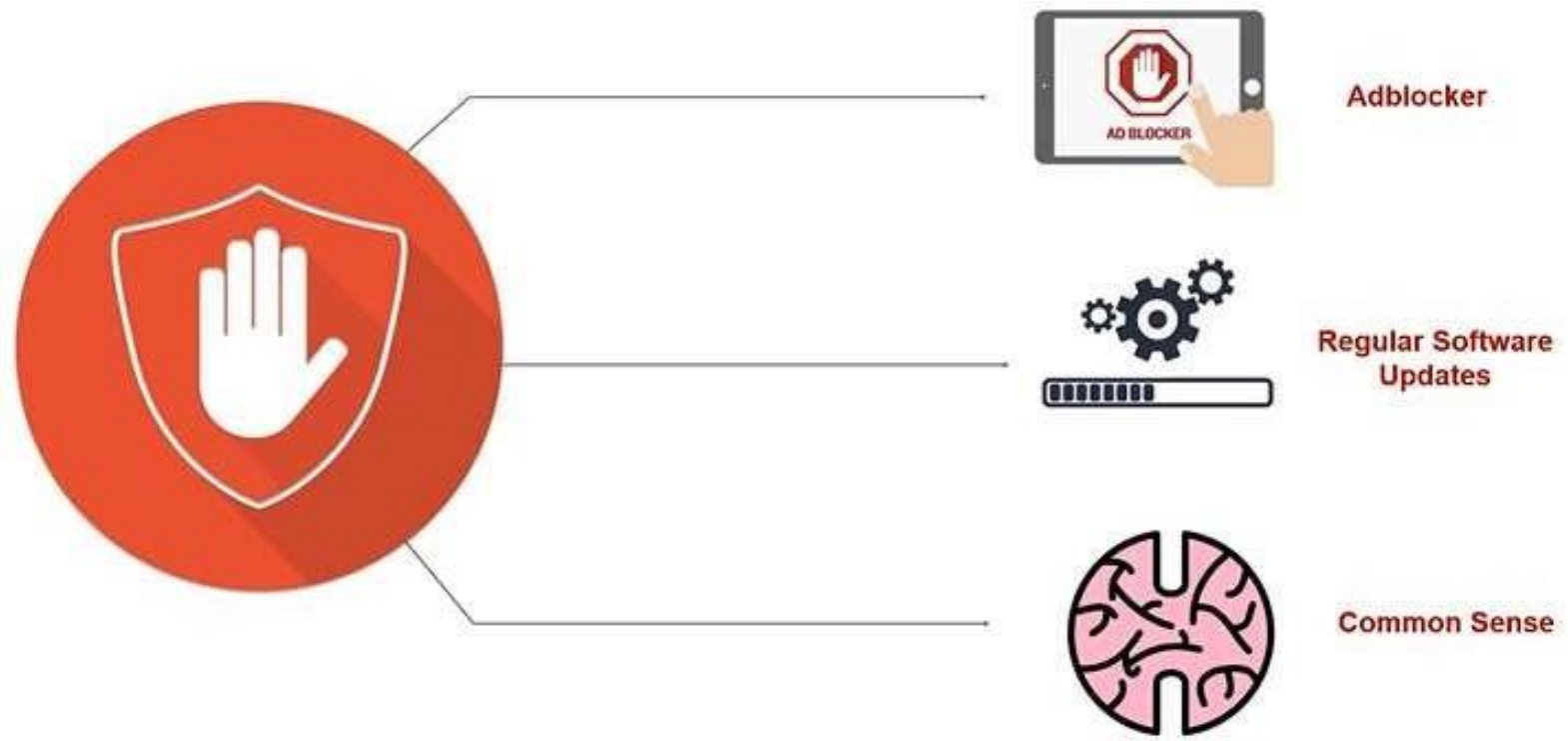
How it work?



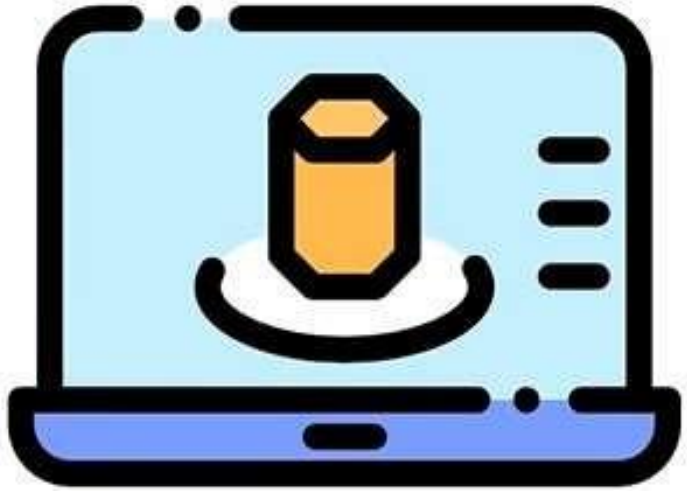
Malvertising

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


AD BLOCKER
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

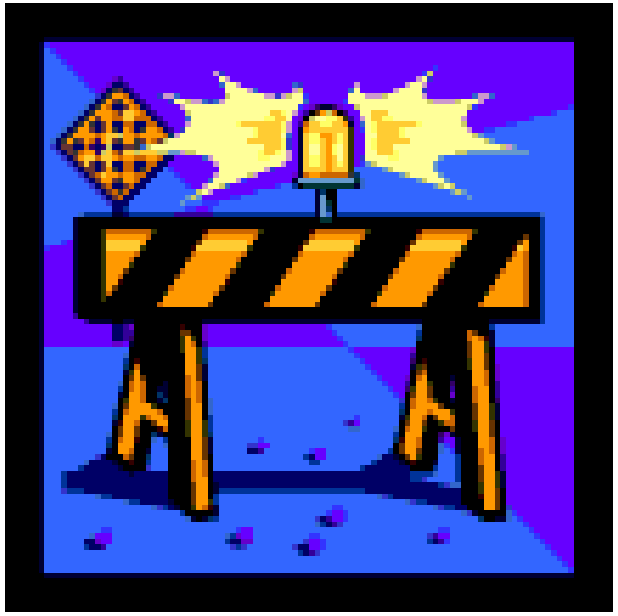
Updated Firewall

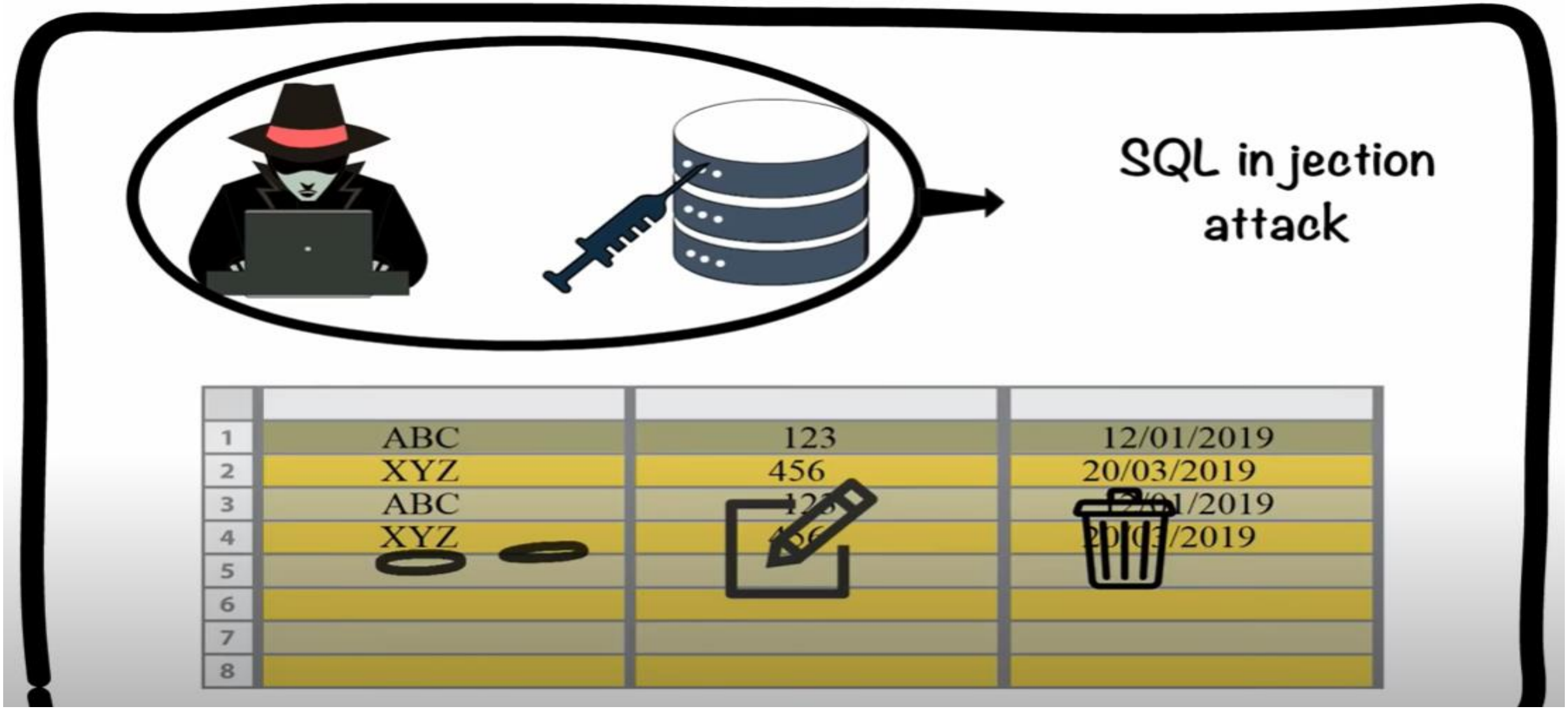
Use Efficient Antivirus

General Distrust

Web Attacks

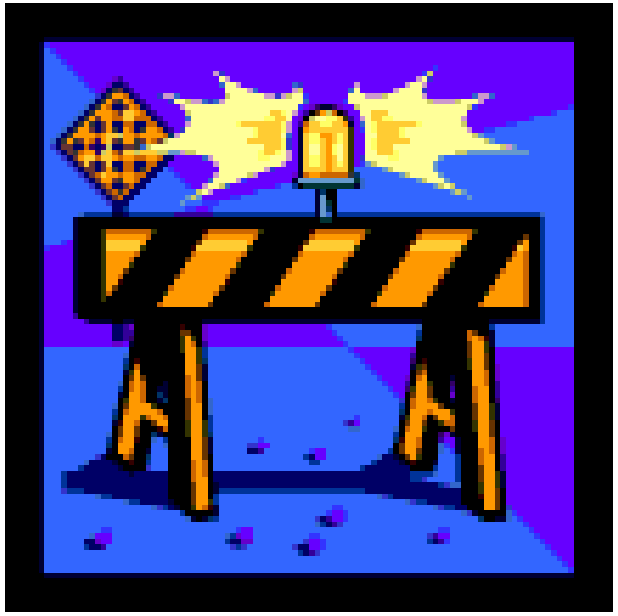
- The attacker attempts to breach a web application. Common attacks of this type are SQL injection




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

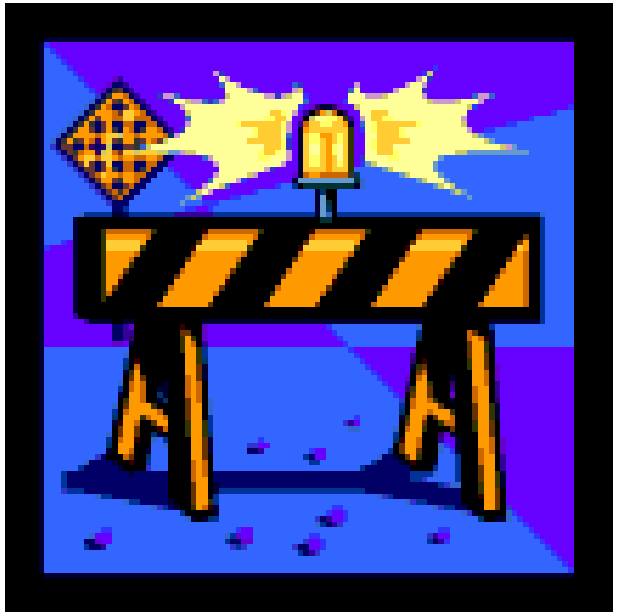
Session Hijacking

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



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.

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 provide 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.)

- 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

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

Basic Security Terminology

People:

- Hackers
  - White hats
  - Black hats
  - Gray hats
- Script kiddies
- Ethical hackers/Sneakers

Basic Security Terminology (cont.)

Devices

- Firewall
  - Filters network traffic
- Proxy server
  - Disguises IP address of internal host
- Intrusion Detection System
  - Monitors traffic, looking for attempted attacks

Basic Security Terminology (cont.)

Activities

- Authentication
- Auditing

Network Security Paradigms

- How will you protect your network?
  - CIA Triangle
  - Least Privileges
  - Perimeter security approach
  - Layered security approach
  - Proactive versus reactive
  - Hybrid security method

How Do Legal Issues Impact Network Security?

- *The Computer Security Act of 1987*
- *OMB Circular A-130*
- See www.alw.nih.gov/Security/FIRST/papers/legal/statelaw.txt for state computer laws
- Health Insurance Portability and Accountability Act of 1996, HIPAA

Online Security Resources

- CERT
  - www.cert.org
- Microsoft Security Advisor
  - www.microsoft.com/security/default.mspx
- F-Secure
  - www.f-secure.com
- SANS
  - www.sans.org

Summary

- Network security is a constantly changing field.
- You need three levels of knowledge.
  - Take the courses necessary to learn the basic techniques.
  - Learn your enterprise system intimately, with all its strengths and vulnerabilities.
  - Keep current in the ever-changing world of threats and exploits.