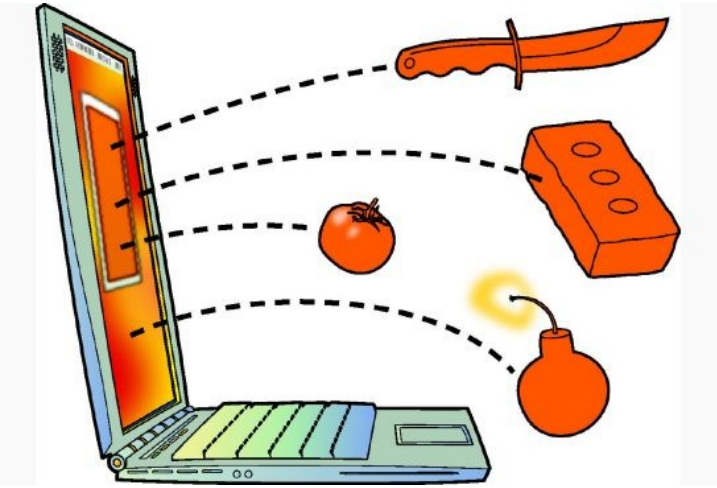
Overview of Cyber CRIMES

Types Of Cyber Crimes

- ***Social Media Websites/ Platform Related Crime***:
  - ***Fake Profile***: Fake profiles are often used to commit cybercrime anonymously or with an untraceable identity.

- ***<u>Cyber Defamation</u>***: Defaming an individual or a company's web site thereby causing embarrassment and also loss.

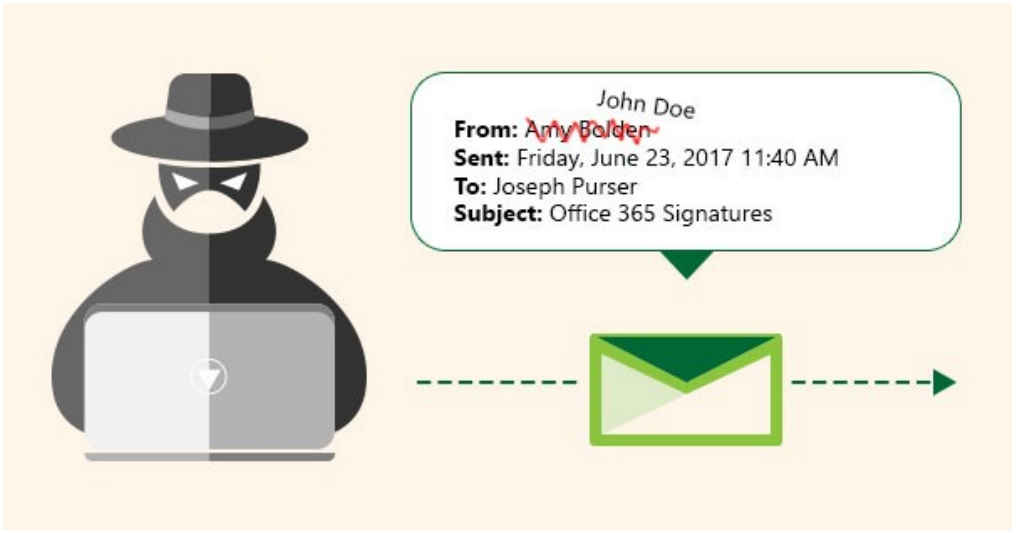


- ***Cyber Stalking***: Repeated acts harassment or threatening behaviour of the cyber criminal towards the victim by using inter- net services.

- ***<u>Cyber Pornography</u>***:Pornography is posting, publishing, and transmitting obscene messages, photographs, videos, and text through e-mail, Web sites, chatting, and other forms over the Internet. Child pornography is one of the biggest ventures on the Internet.

- ***E-mail Related Crimes***:

➢ ***E-mail Spoofing***: Messages from the fraudster appearing to be from a genuine source (like bank), seeks personally identifiable information to perpetrate fraud on the victim.



- ***Phishing***: Using spoof E-mails or directing the people to fake web sites to deceive them into divulging personal financial details so that criminals can access their accounts.

- ***E-mail Bombing***: Email bombing is sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

- ***Spamming***: Sending unsolicited mails and messages.

- ***E-mail Frauds:*** Intentional deception made for personal gain or to damage another individual through email.

- ***Examples:***

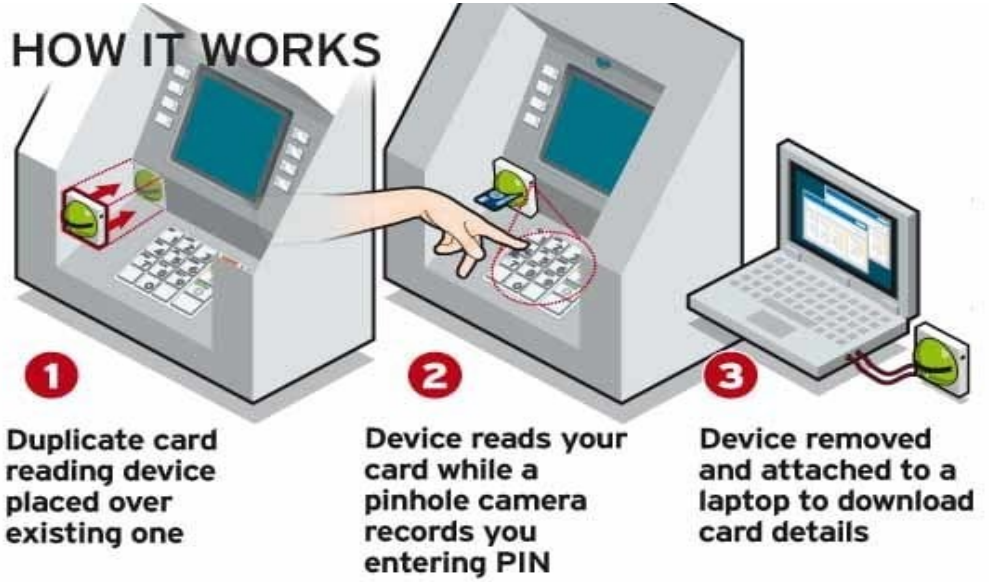
- Nigerian frauds
- Investment Schemes frauds
- Job frauds
- Lottery frauds
- E-mail Spoofing
- Phishing
- E-mail Bombing
- Chain mail frauds.

- ***Financial Crimes***

➢ ***Debit/Credit Card Frauds***: The unauthorized use of an individual's credit card or card information to make purchases, or to remove funds from the cardholder's account.

➢ ***Example***:

- Skimming is a kind of credit/debit/ATM/chip/SIM card fraud in which a hand-held device called skimmer is used to capture the information contained in it.
- The data can be transferred on to a computer system later. The information like name, credit card number, expiry date, etc., can be used to create fake credit cards.



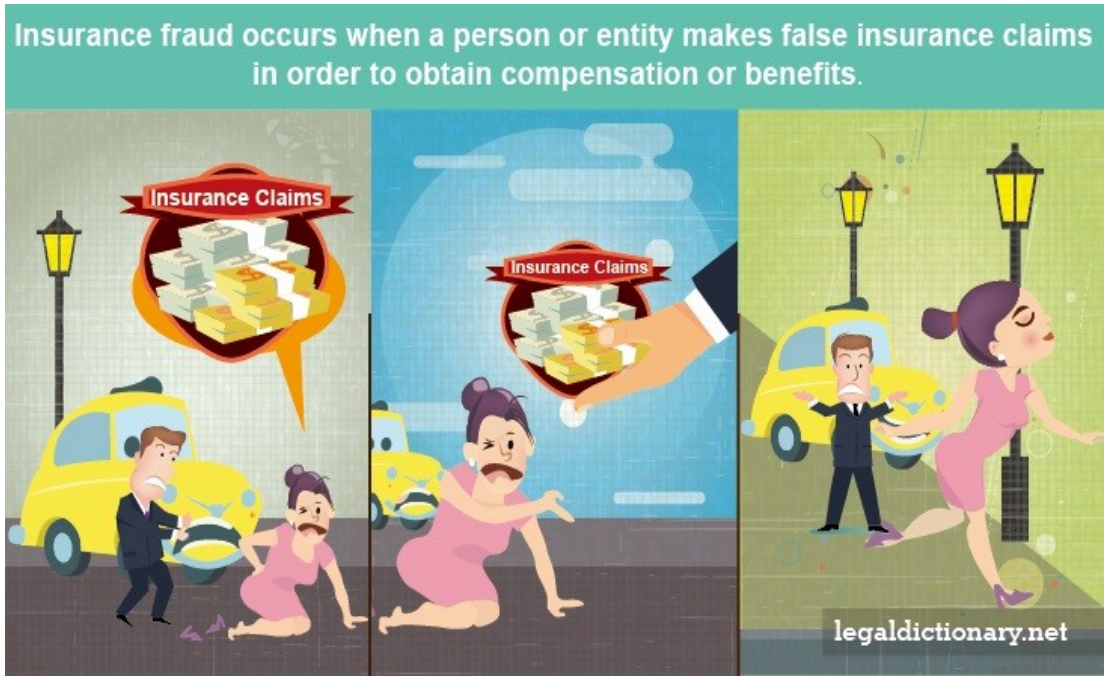
- ***Illegal Online Transactions***: Payment fraud is any type of false or illegal transaction completed by a cybercriminal. The perpetrator deprives the victim of funds, personal property, interest or sensitive information via the Internet.

➢ ***Job Frauds***:

- Job fraud occurs when a scammer poses as an employer or recruiter, and offers attractive employment opportunities which require that the job seeker pay money in advance.

- ***Lottery Frauds:*** A type of advance-fee fraud which begins with an unexpected email notification, phone call, or mailing (sometimes including a large check) explaining that "You have won!" a large sum of money in a lottery.

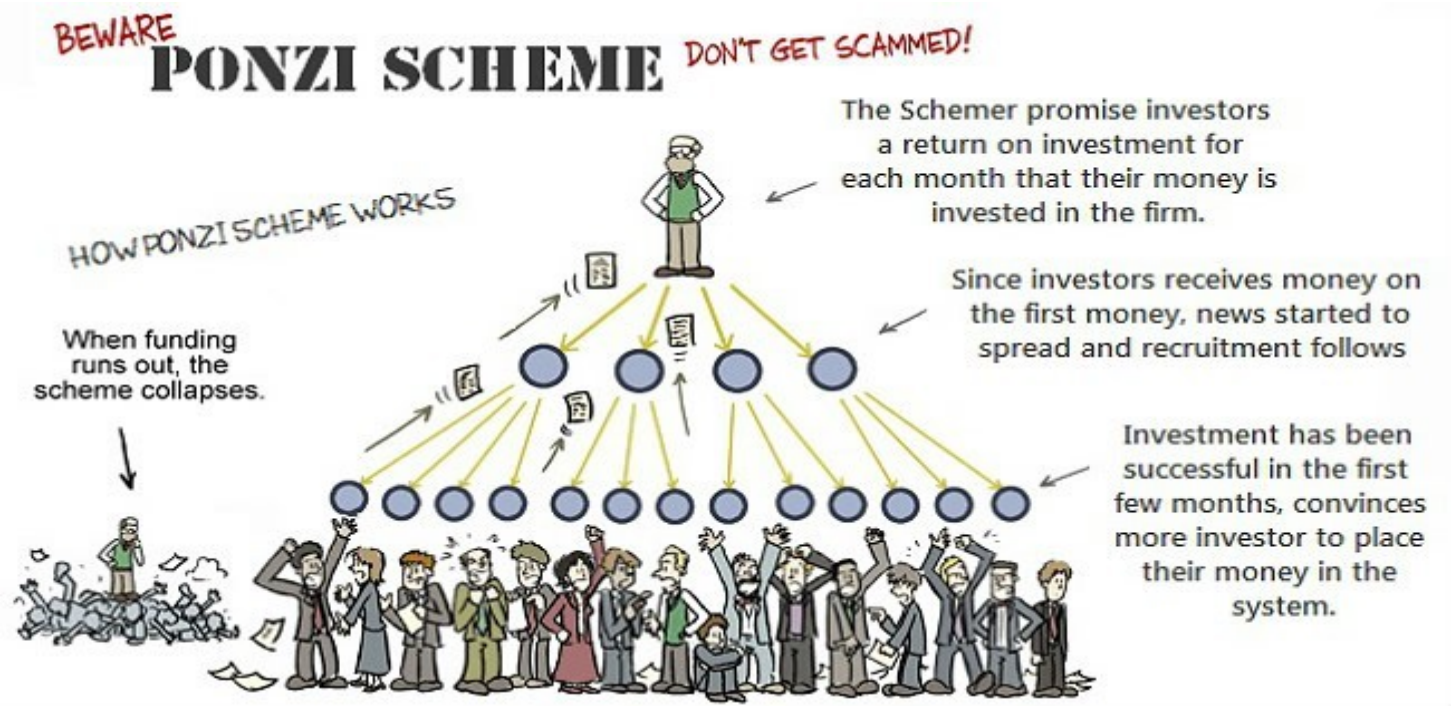
- ***<u>Insurance Frauds</u>***: When someone provides false information to an insurance company in order to gain something of value that he or she would not have received if the truth had been told, they've committed insurance fraud.



➢ ***<u>Ponzi scheme Fraud</u>***:

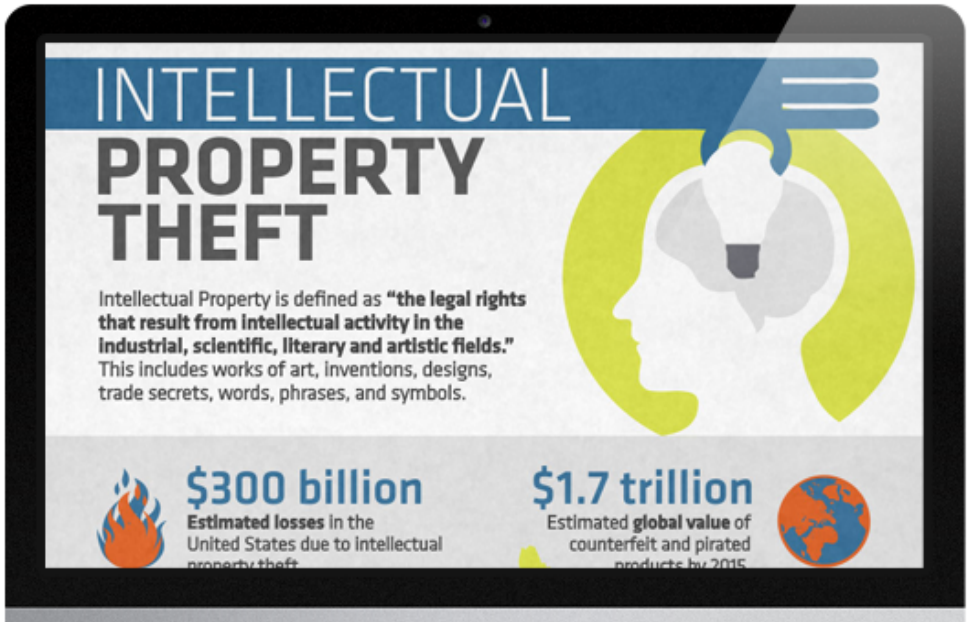
- fake investment that one schemer (or group of schemers) gets other people to give money to.
- "I found a great way to make money fast. The more you give me, the more I can invest in that cause, and the more I can earn for us all".
- These schemes always stop one of three ways:

1. The schemer runs away with the money they got. This is what schemers try to do.
2. The schemer runs out of money; They will be unable to promise money back right away. This is called *liquidity*, and makes investors panic and demand their money back, often all at once.
3. Authorities (or sometimes whistleblowers on the inside) find out about the scheme and stop it.

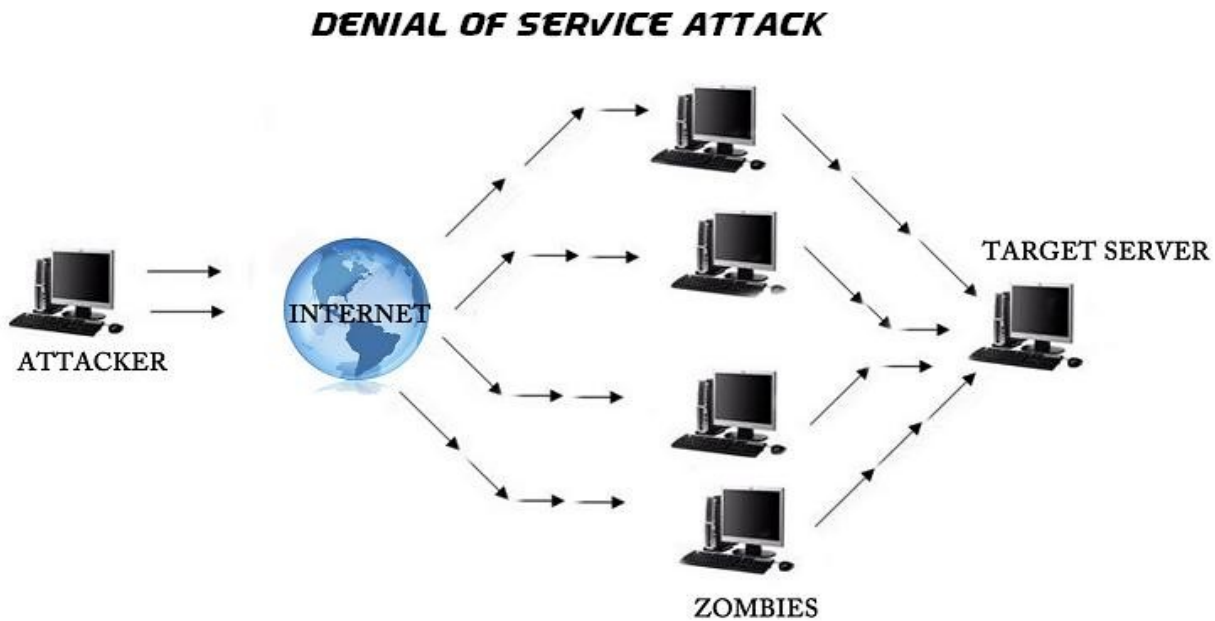


- ***Other Cyber Crimes***
  - ***Hacking:*** Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network.

- ***Intellectual Property Right Violation:*** Intellectual property (IP) theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations.



- ***<u>DOS/D-DOS Attacks</u>***: It is a multitude of compromised systems attack a single target computer, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.



- ***Virus/Worm Attacks***: **:** A self-replicating program that runs and spreads by modifying other programs or files / A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

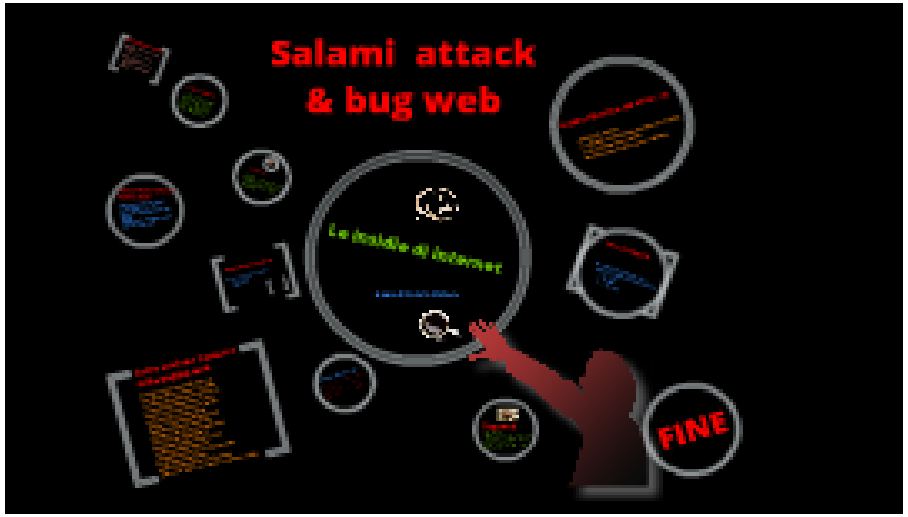
- ***<u>Malware Attacks</u>***: : A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

- ***Spywares***: It is a type of malware that is secretly or surreptitiously installed into an information system to gather information on individuals or organisations without their knowledge; a type of malicious code.

- ***Cyber Pornography***:Pornography is posting, publishing, and transmitting obscene messages, photographs, videos, and text through e-mail, Web sites, chatting, and other forms over the Internet. Child pornography is one of the biggest ventures on the Internet.

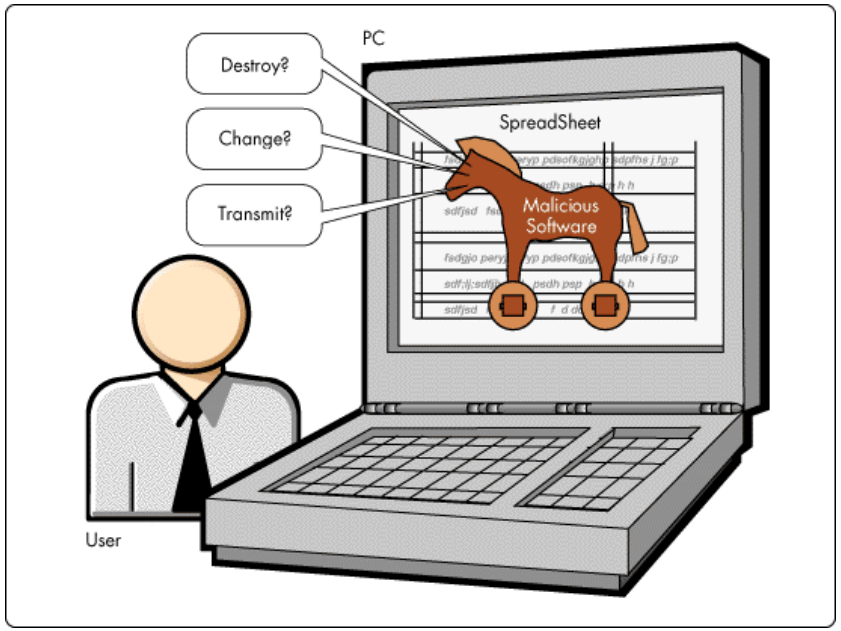
- ***Web Defacement***: Attack on a **website** that changes the visual appearance of the site or a webpage. These are typically the work of defacers, who break into a **web** server and replace the hosted **website** with one of their own.

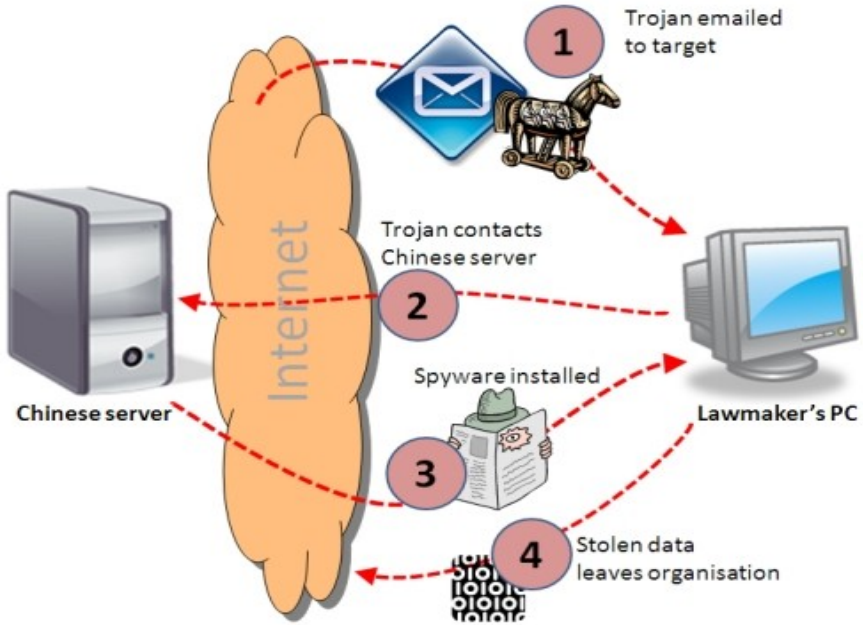
- ***Salami Attack***: A programmed attack which is implemented in small (meant to be unnoticeable) increments. This attack involves making alteration so insignificant that it is easily concealed and would go completely unnoticed. Attacks are used for commission of financial crimes.



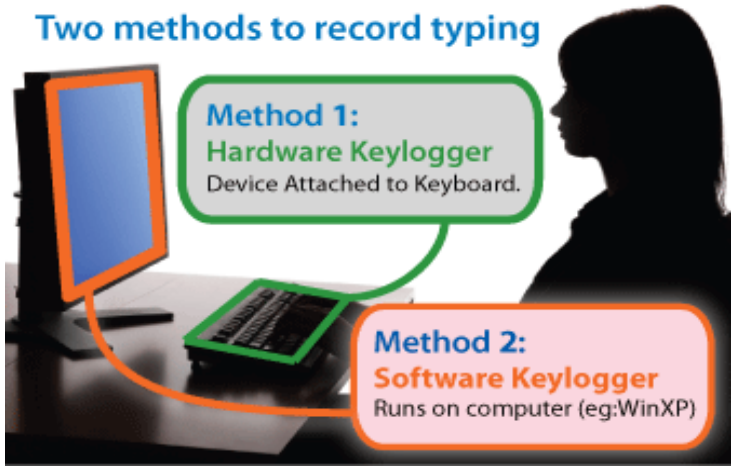
- ***Internet Time Theft***: It is the use by an unauthorised person, of the Internet hours paid by another person. The person who gets access to someone else's ISP user ID & password, either by hacking or gaining access by illegal means and using it to gain access without the other person's knowledge.

- ***Trojan***: A malicious program that masquerades as a benign application and can take complete control of the victim's computer system.



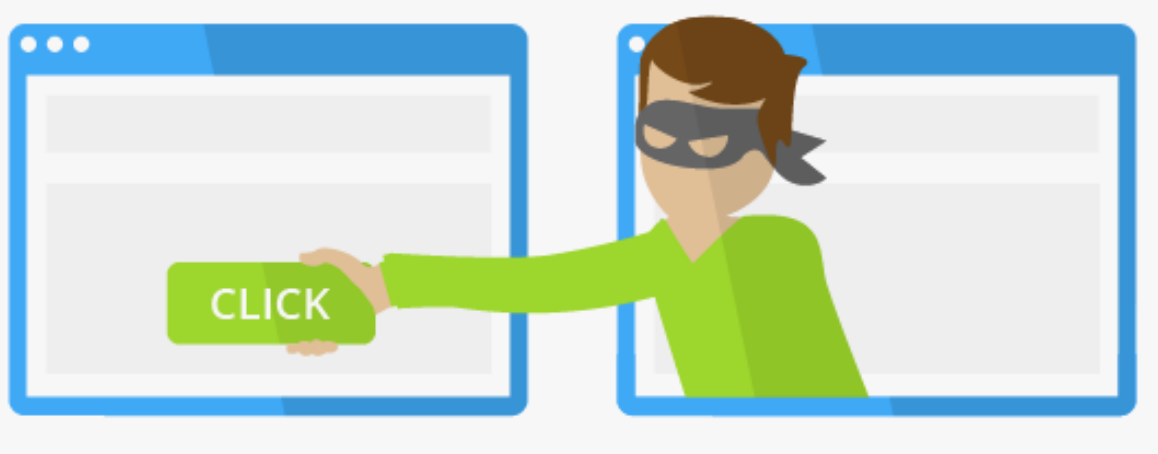


- ***Key Logger***: A computer program that records every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information.



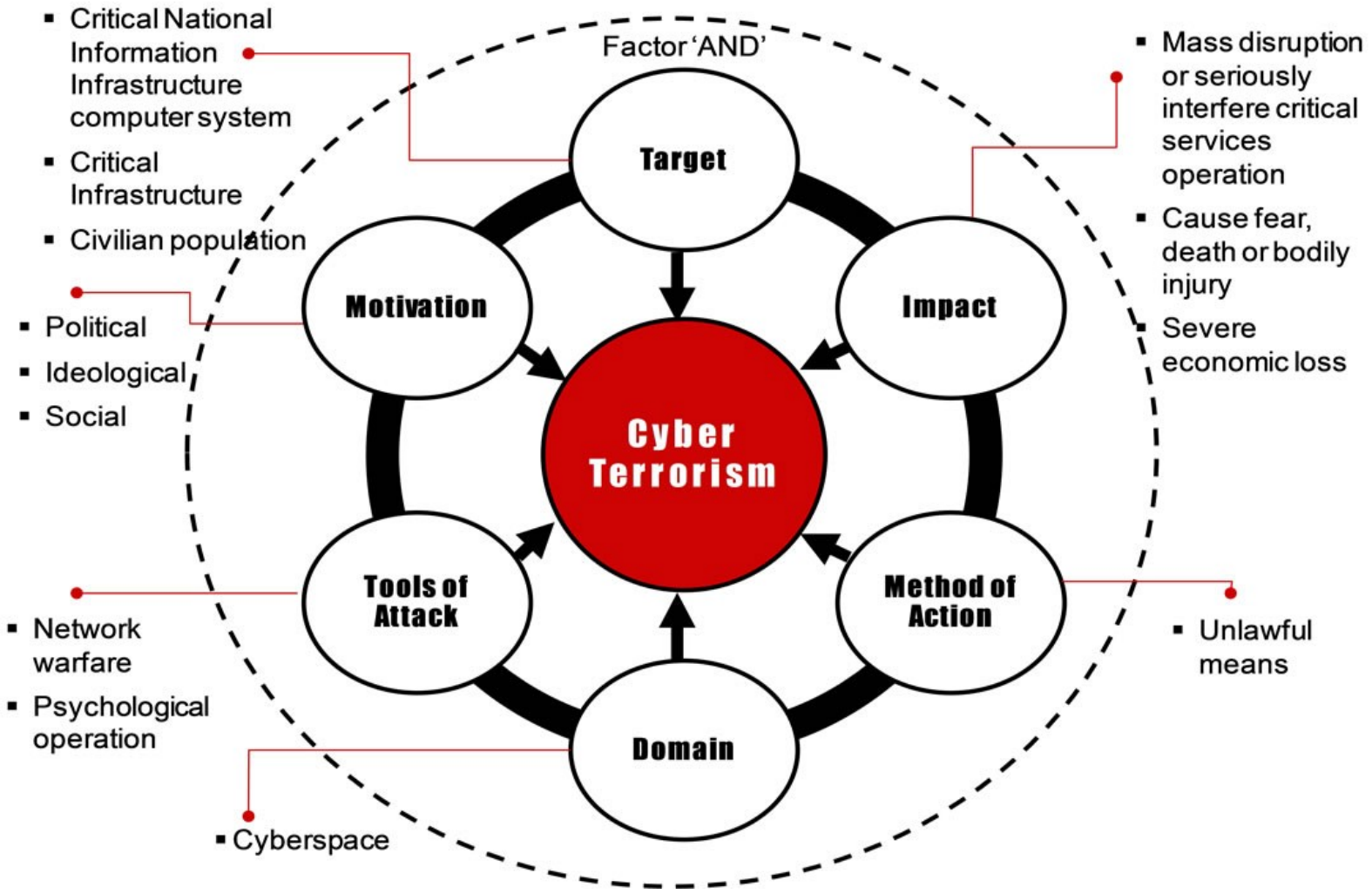
- ***Online Sale Of Illegal Articles***:It is becoming increasingly common to find the illegal where sale of narcotics drugs, weapons, wildlife etc. is being facilitated by the internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc.

- ***Web Jacking***: Occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.



➢ ***Cyber Terrorism***:

- Use of the internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political gains through intimidation.
- Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.



- ***<u>Case Study:</u>***

- On November 26 2010, a group calling itself the Indian Cyber Army hacked the websites belonging to the Pakistan Army, Ministry of Foreign Affairs, Ministry of Education, Ministry of Finance, Pakistan Computer Bureau, Council of Islamic Ideology, etc. The attack was done as a revenge for the Mumbai terrorist attacks.

Glossary of Cyber Crimes TERMS

- **Data** - Information in analog or digital form that can be transmitted or processed.
- **Data Extraction** - A process that identifies and recovers information that may not be immediately apparent.
- **Encryption** - procedure that converts plain text into symbols to prevent anyone but the intended recipient from understanding the message
- **Forensic Wipe** - A verifiable procedure for sanitizing a defined area of digital media by overwriting each byte with a known value; this process prevents cross-contamination of data.
- **Handheld (Mobile) Devices** - Handheld devices are portable data storage devices that provide communications, digital photography, navigation systems, entertainment, data storage, and personal information management.
- **Hash or Hash Value** - Numerical values that represent a string of text (search term), generated by hashing functions (algorithms). Hash values are used to query large sums of data such as databases or hard drives for specific terms. In forensics, hash values are also used to substantiate the integrity of digital evidence and/or for inclusion and exclusion comparisons against known value sets.
- **Media** - Objects on which data can be stored. Includes hard drives, thumb drives, CD/DVD, floppy discs, SIM cards from mobile devices, memory cards for cameras, etc.
- **Metadata** - Data, frequently embedded within a file, that describes a file or directory, which can include the locations where the content is stored, dates and times, application specific information, and permissions. Examples: Email headers and website source code contain metadata.
- **Partition** - User defined section of electronic media. Partitions can beused to separate and hide information on a hard drive.

- **Write Block/Write Protect -** Hardware and/or software methods of preventing modification of content on a media storage unit like a CD or thumb drive.
- **Log File -** A record of actions, events and related data.
- **File Format –** Structure by which data is organised.