INFORMATION SECURITY AND CYBER LAW

BY SUCCESS SHRESTHA

Digital Society

- A digital society is a modern, progressive society that is formed as a result of adoption and integration of Information and Communication Technologies at home, work, education and r0ecreation
- Every aspect of digital society is profoundly being affected by the digitalization of data
- Digital solutions allow a more efficient use of resources and products can be customized to a degree that was unreachable only a few years ago

COMPUTER ETHICS

- Ethics is a set of moral principles that govern the behavior of an individual or group of people
- Computer ethics deals with the procedures, values and practices that govern the process of consuming computing technology and its related disciplines without damaging or violating the moral values and beliefs of any individual, organization or entity
- Computer ethics is a concept in ethics that addresses the ethical issues and constraints that arise from the use of computers, and how they can be mitigated or prevented
- It includes methods and procedures to avoid infringing copyrights, trademarks and the unauthorized distribution of digital content

Ten commandment of computer ethics defined by Computer Ethics institute in 1992

1) You shall not use a computer to harm other people

2) You shall not interfere with other people's computer work

3) You shall not snoop around in other people's files

4) You shall not use a computer to steal

5) You shall not use a computer to bear false witness

6) You shall not use or copy software for which you have not paid

7) You shall not use other people's computer resources without authorization

8) You shall not appropriate other people's intellectual output

9) You shall think about the social consequences of the program you write

10) You shall use a computer in ways that show consideration and respect:

INFORMATION SECURITY (InfoSec)

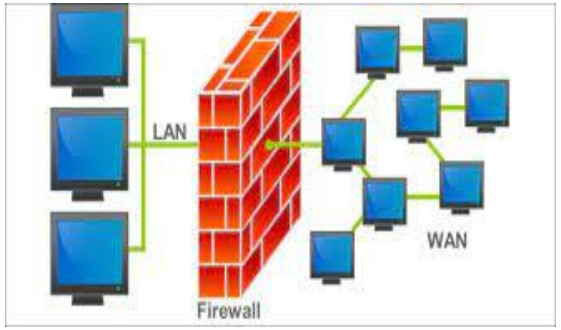
- Information security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information
- Enables organizations to protect digital and analog information
- Provides coverage for cryptography, mobile computing, social media, as well as infrastructure and networks containing private, financial, and corporate information
- Protecting information by mitigating information risks

THREATS TO INFORMATION SECURITY

- Unintentional threats
  - Done by mistake
  - Unknown error
  - Some testing faults
- Intentional threats
  - These are crimes
  - Punishment are given
  - Phishing, ransomware, virus, logic bomb , etc

INFORMATION SECURITY MEASURES

- Authentication
- Backup
- Antivirus
- Firewall
- Cryptography
- Physical Control



Now explain all of these and bring on next class otherwise Diable Jamble Kick

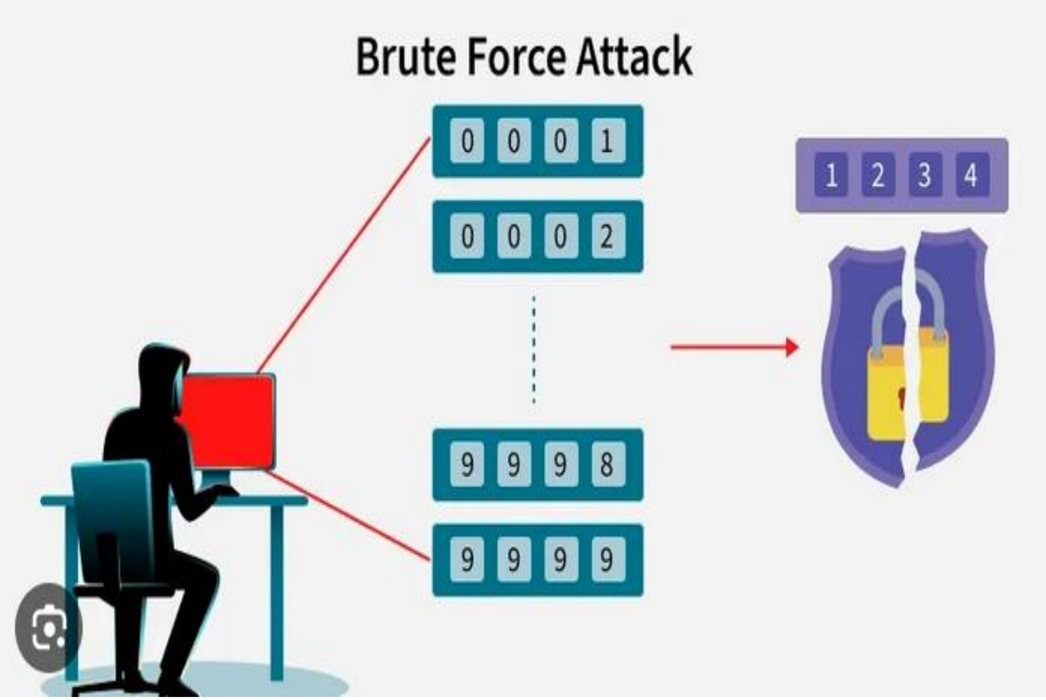
Cyber Crime

- Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.
- cybercrime is committed by cybercriminals or hackers who want to make money
- Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of a crime
- Unauthorized access to or modification of data or application
- Viruses and Malware, Identity Theft, Hacking, Phishing

TYPES OF CYBER CRIME

Trespass

- Trespass is a legal term referring to the unauthorized entry onto another person's property, or interference with their property rights, and is generally considered a civil wrong, though it can sometimes be a criminal offense.
- **Brute force attack** is a trial-and-error method used to obtain unauthorized access to accounts, systems, or encrypted data by systematically guessing passwords, login credentials, or encryption keys until the correct one is found



TYPES OF CYBER CRIME

Information Extortion

- Information extortion (or cyber extortion) is a malicious act where attackers steal, encrypt, or threaten to expose sensitive data to blackmail individuals or organizations into paying a ransom
- Common tactics include ransomware, DDoS attacks, and doxing, often demanding payment in cryptocurrency. Victims face reputational damage, financial loss, and service disruption, with no guarantee of data recovery even if the ransom is paid

TYPES OF CYBER CRIME

Identity Theft

- Identity theft in cybersecurity is the unauthorized acquisition and use of personal data—such as Social Security numbers, passwords, and bank details—to commit fraud, financial theft, or impersonation
- Perpetrators use techniques like phishing, malware, and data breaches to steal credentials for illicit gain, leading to severe financial, legal, and reputational damage for victim
- Victims may face drained bank accounts, ruined credit scores, legal issues from crimes committed in their name, and long-term recovery efforts.

TYPES OF CYBER CRIME

Piracy

- Piracy refers to either violent robbery on the high seas or the illegal, unauthorized reproduction and distribution of copyrighted intellectual property
- Unauthorized copying or distribution of copyrighted software.
- Accessing copyrighted content without paying, often via unauthorized websites or apps

TYPES OF CYBER CRIME

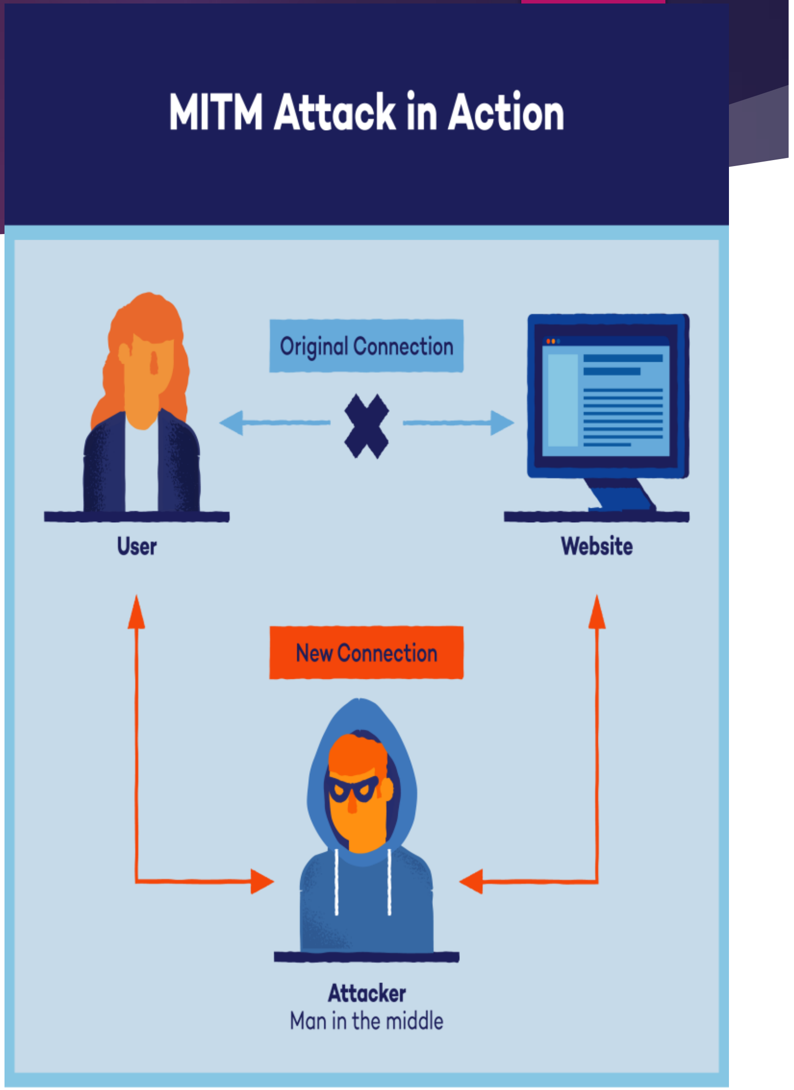
Cyber terrorism

- Cyber terrorism is the premeditated, ideologically or politically motivated attack against information, computer systems, and data by sub-national groups or clandestine agents to induce fear, cause real-world harm, or disrupt critical infrastructure
- Critical infrastructure (power grids, transportation, banking), government systems, and public communication networks.

TYPES OF CYBER CRIME

Man in the middle Attack

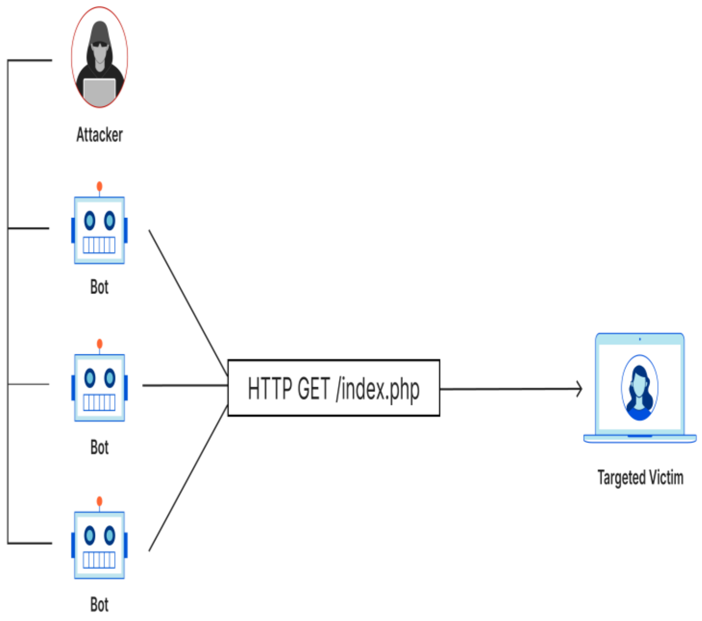
- A Man-in-the-Middle (MitM) attack is a cyberthreat where an attacker secretly inserts themselves between two parties (e.g., a user and a website) to intercept, steal, or alter data in transit.
- The attacker acts as a proxy, eavesdropping on or modifying communication, often without either party realizing.



TYPES OF CYBER CRIME

DOS

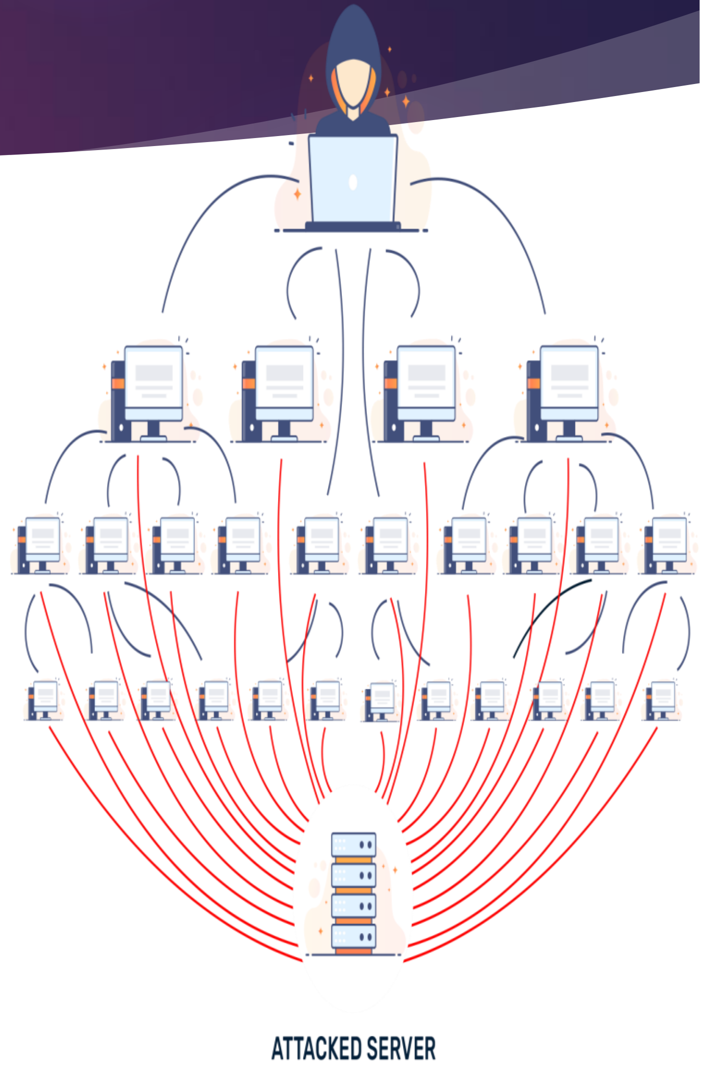
- A Denial-of-Service (DoS) attack disrupts or shuts down websites, servers, or network resources by overwhelming them with fraudulent traffic, creating a "traffic jam" that makes them unusable
- Attackers send excessive, malformed, or spoofed requests (e.g., HTTP floods, UDP packets).
- Websites become slow, unresponsive, or crash entirely, resulting in interrupted service, lost revenue, and, in some cases, a smokescreen for other attacks like ransomware



TYPES OF CYBER CRIME

DDOS

- A Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt a server, service, or network by overwhelming it with a flood of Internet traffic from multiple compromised systems (botnets)
- These attacks target application resources, causing slow performance or complete downtime for legitimate users, impacting industries like gaming, e-commerce, and finance



TYPES OF CYBER CRIME

Social Engineering Attack

- Social engineering in cybersecurity is the psychological manipulation of people into performing actions or divulging confidential information, exploiting human error rather than software vulnerabilities
- Typically involves four stages: investigation (gathering information), hooking (initiating contact), playing (manipulating the victim), and exiting (covering tracks).

Cyber Bullying

- Cyberbullying or cyber harassment is a form of bullying or harassment using electronic means
- Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else
- Cyberbullying can result in increased distress for the victims along with increased anger and frustration
- The internet and mobile phones have such positive potential to transform children's lives for the better

Malicious Software

- Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server
- Leak private information, gain unauthorized access to information or systems, deprive users access to information or which unknowingly interferes with the user's computer security and privacy
- According to Symantec’s 2018 Internet Security Threat Report (ISTR), there are 669,947,865 malwares in 2017
- Worms, Trojan Horse, Logic Bomb, Ransomware, etc are examples of malware software

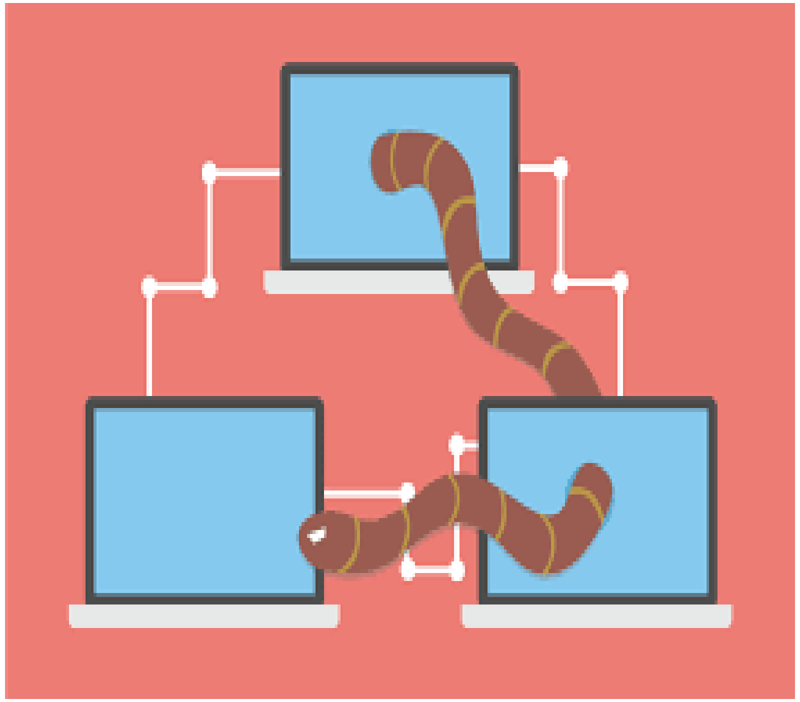
Some malware software

- Worms
- Trojan Horse
- Logic Bomb
- Ransomware
- Adware
- Spyware

Explain All

Malware Software:

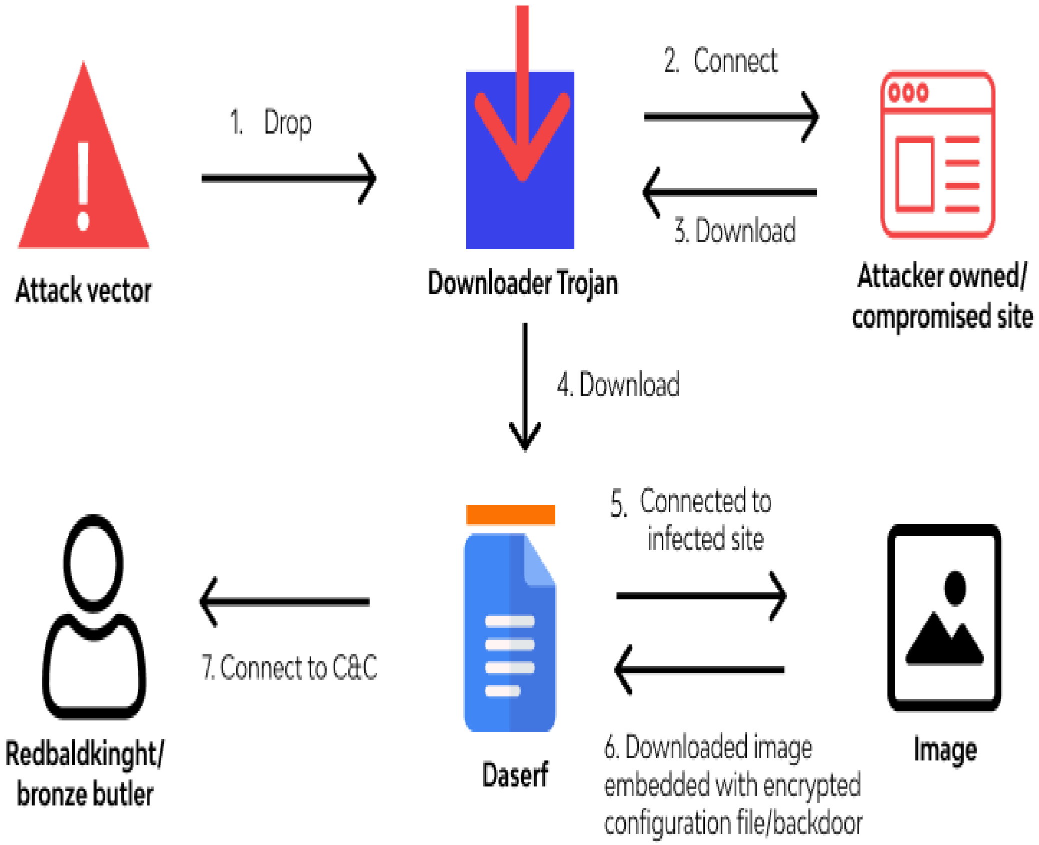
- A **worm** is a type of malware that can copy itself and spread automatically from one computer to another through networks (internet, Wi-Fi, USB, etc.) without user action. It can slow down networks and damage systems.
- A worm is a virus that spreads by itself.
- A computer in a cyber café in Kathmandu gets infected and the worm spreads to all connected computers through the same Wi-Fi.



Malware Software:

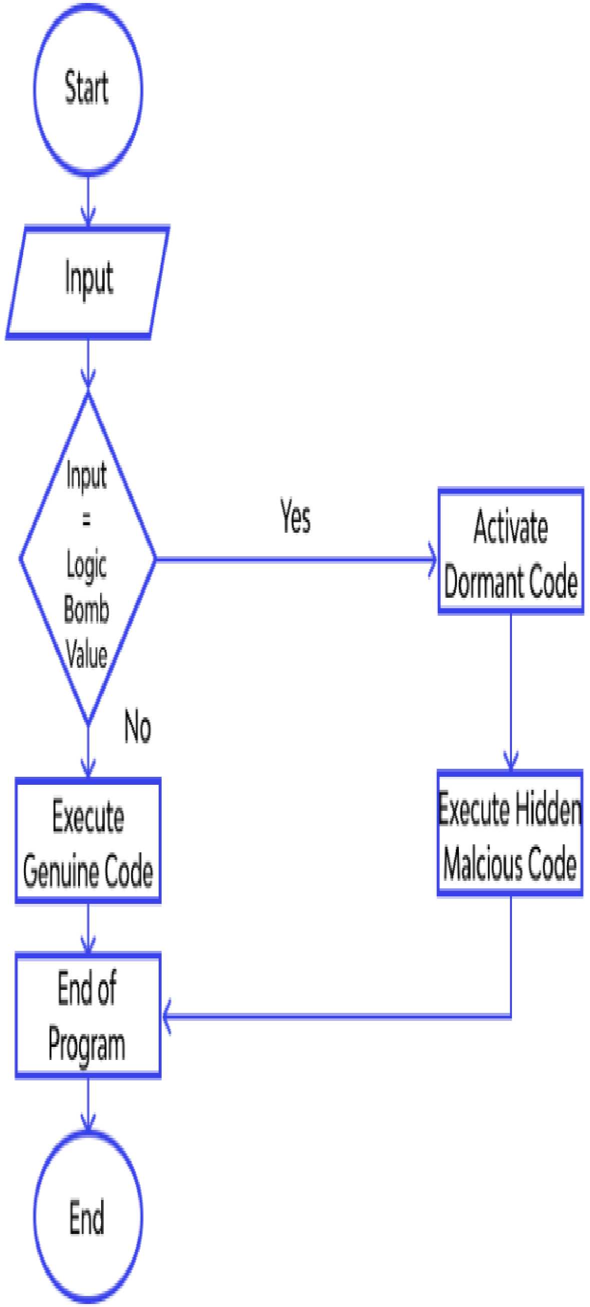
- A **Trojan Horse** is malware that looks like a useful or safe file (game, software, movie) but secretly installs harmful programs when opened. It does not spread by itself and needs the user to run it.
- A Trojan is a fake file that harms your computer when you open it.
- Someone downloads a "free movie" from a random website, but after opening it, their Facebook account gets hacked.

Example of how "Daserf" Trojan works


Attack vector
1. Drop
Downloader Trojan
2. Connect
3. Download
Attacker owned/ compromised site
4. Download
5. Connected to infected site
6. Downloaded image embedded with encrypted configuration file/backdoor
Image
Daserf
7. Connect to C&C
Redbaldkinght/ bronze butler

Malware Software:

- A **Logic Bomb** is a hidden malicious code that activates only when a specific condition is met (like a date, time, or action). Until then, it stays silent inside the system.
- A logic bomb is a virus that attacks later at a fixed time or condition.
- A fired employee sets a logic bomb that deletes office files on New Year’s Day.



RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost

Malware Software:

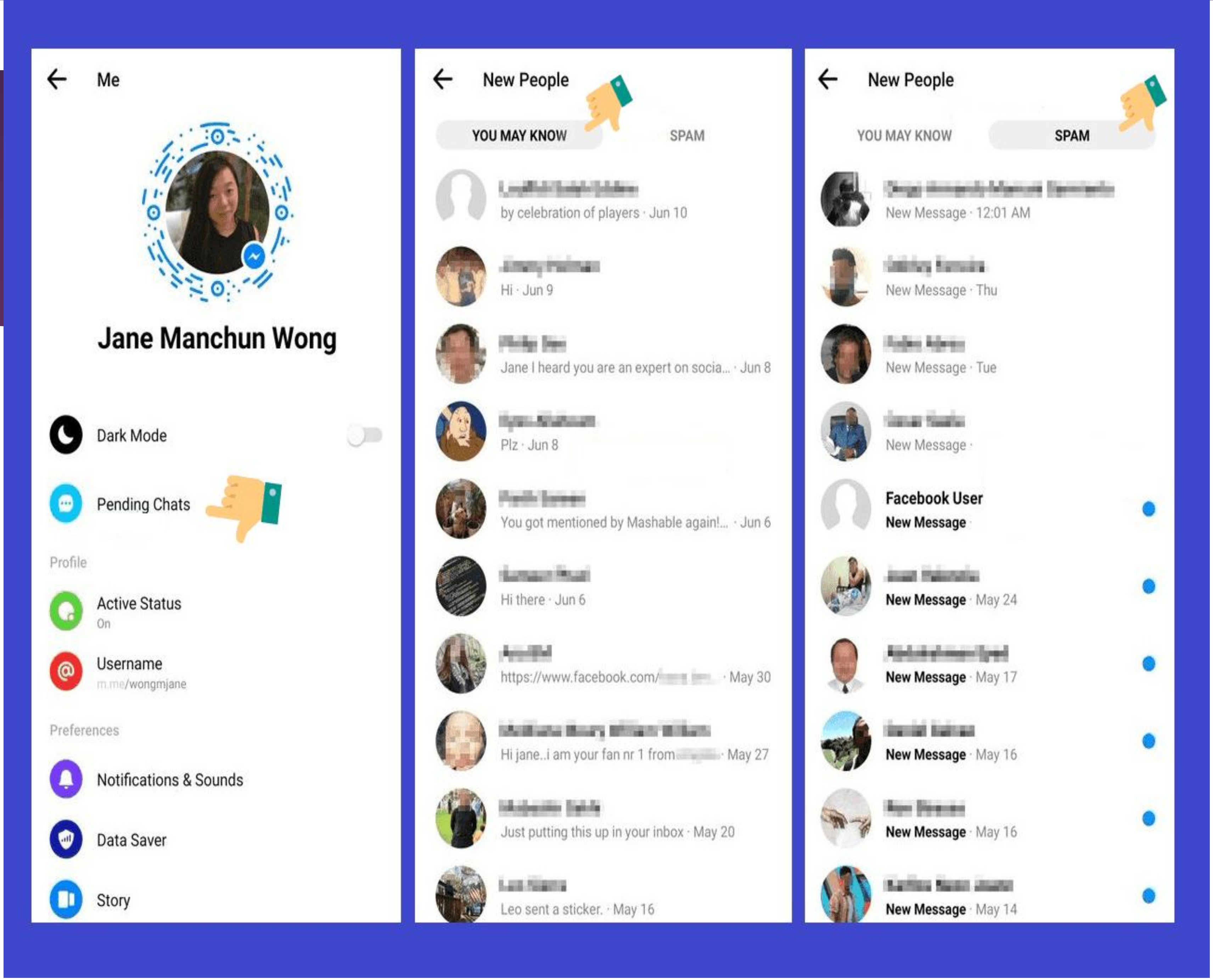
- **Adware** automatically shows unwanted advertisements on your device. It may track browsing behavior and slow down the system. Some adware installs with free apps.
- Adware shows too many ads on your screen.
- After installing a free game, many pop-up ads appear while browsing websites.

Malware Software:

- **Spyware** secretly collects user information like passwords, browsing history, messages, and sends it to hackers without the user knowing.
- Spyware secretly watches what you do on your computer.
- A user logs into eSewa on an infected computer and their password gets stolen.

Spam

- Spam is digital junk mail, unsolicited communications sent in bulk over the internet or through any electronic messaging system
- Spam is unsolicited message sent to multiple recipient
- There may be virus or some sort of software program which does it work automatically similarly like malware software



[redacted] by celebration of players · Jun 10

[redacted] Hi · Jun 9

[redacted] Jane I heard you are an expert on socia... · Jun 8

[redacted] Plz · Jun 8

[redacted] You got mentioned by Mashable again!... · Jun 6

[redacted] Hi there · Jun 6

[redacted] https://www.facebook.com/[redacted] · May 30

[redacted] Hi jane..i am your fan nr 1 from[redacted] · May 27

[redacted] Just putting this up in your inbox · May 20

[redacted] Leo sent a sticker. · May 16

[redacted] New Message · 12:01 AM

[redacted] New Message · Thu

[redacted] New Message · Tue

[redacted] New Message ·

Facebook User New Message ·

[redacted] New Message · May 24

[redacted] New Message · May 17

[redacted] New Message · May 16

[redacted] New Message · May 16

[redacted] New Message · May 14

Protection from Cyber Crime

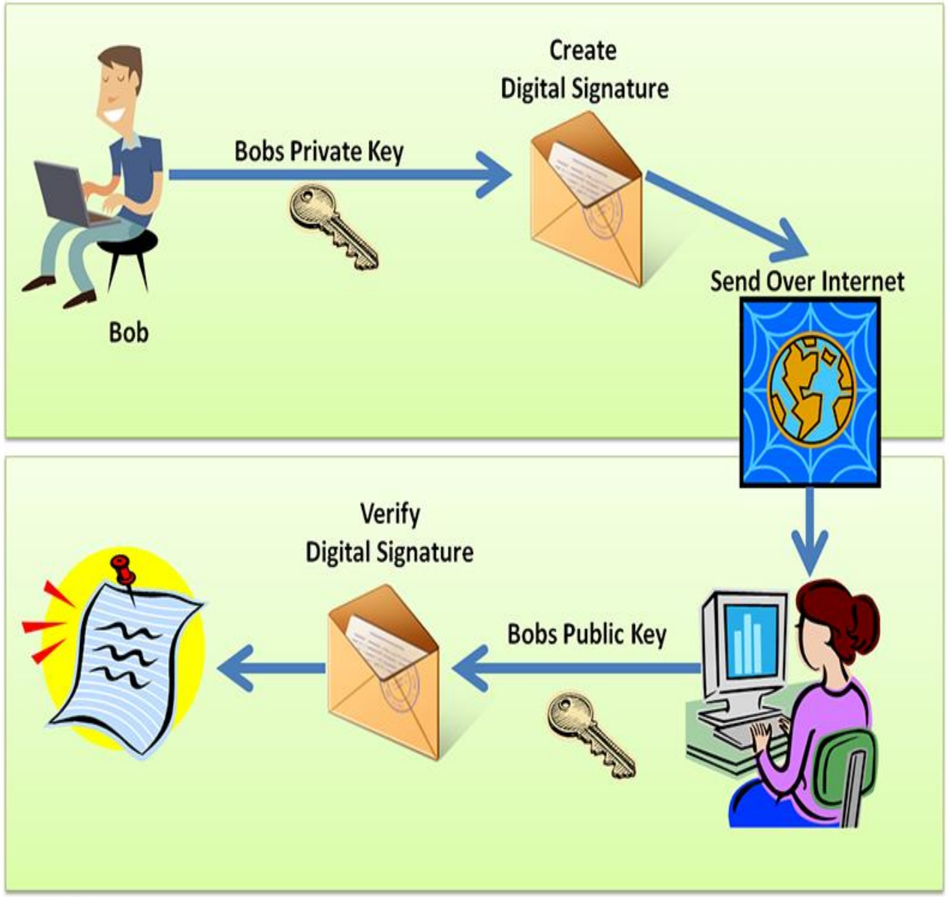
- Use trusted antivirus and keep it updated to detect malware.
- Always update Windows, Android, and apps to fix security bugs.
- Avoid clicking random links on Facebook, Messenger, email, or SMS.
- Don't download movies, games, or software from unknown sites.
- Use long passwords with letters, numbers, and symbols.
- Never share your Facebook, Gmail, or eSewa passwords with anyone.
- Turn on OTP or verification codes for social media and email.

Protection from Cyber Crime

- Don’t log in to banking or wallets on free public Wi-Fi.
- Always scan pen drives to avoid worms and viruses.
- Use Google Play Store or App Store, not third-party APK sites.
- Don’t open unknown files like .exe, .zip, or fake invoices.
- Save copies of files to cloud or external drive
- Keep your device firewall turned ON for network protection.
- Always log out after using cyber cafés or school computers.
- Stay aware of cyber crimes and teach friends/students basic safety rules.

Digital signature

- A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.
- It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security
- A digital signature is like an electronic fingerprint used to verify that a message or document is really from the sender.
- It ensures the authenticity of the sender and proves the message was not tampered with.
- Digital signatures use encryption techniques (like public and private keys) to secure data.
- It provides integrity, meaning the information cannot be changed without detection.
- Digital signatures are widely used in emails, online transactions, and e-documents to make them trustworthy.



Cyber law in Nepal

- Nepal is developing towards ICT (Information and Communication Technology) rapidly due to this we may face various criminal activities done by using computer
- Most of business organization, school, hospital, etc are using IT for their support in their daily work and many cheaters are evolving to misuse their data
- **The Electronic Transaction Act, 2063** is Nepal's first cyber law. It was created in response to the growing usage of the internet in Nepal
- It makes provision for the commercial use of computers and networks; authorizes e-transactions and communication in public and private sectors; criminalizes different computer related unwanted activities
- There are all together 6 Chapter and total 42 articles

Cyber law 2063 address focus on following aspect

- The Electronic Transaction Act (ETA), 2063 (2008), is Nepal's primary legislation governing digital activities, providing legal recognition to electronic records, signatures, and transactions.
- It establishes the Office of Certificate Control, regulates Certifying Authorities (CAs), and defines cybercrimes (e.g., hacking, data theft) with penalties ranging from fines to 3-year imprisonment
- Punish hackers who download, copy and manipulate data without permission of owner
- Provision for controlling and verifying the authorities to use digital data
- Legal provision for online banking, electronic fund transfer (EFD)
- Use provision to use digital signature which is essential to identify and verify documents
- People can appeal judicial body to listed the cyber crime related issues

Electronic Transaction Act

- **Cybercrime Provisions & Penalties**
- The Act specifies punishments for several offenses under Cyber Laws in Nepal:
- **Section 47 (Illegal Publication):** Publishing or displaying "obscene" or "harmful" content online can lead to a fine of up to **Rs. 100,000** and/or up to **5 years** of imprisonment.
- **Unauthorized Access (Hacking):** Accessing computer systems without permission is punishable by up to **3 years** in jail or a **Rs. 200,000** fine.
- **Source Code Alteration:** Tampering with or stealing computer source code carries a penalty of up to **3 years** imprisonment or a fine of **Rs. 200,000**.
- **Computer Fraud:** Creating or using fake digital signatures can lead to significant fines and jail time.

Intellectual Property Right

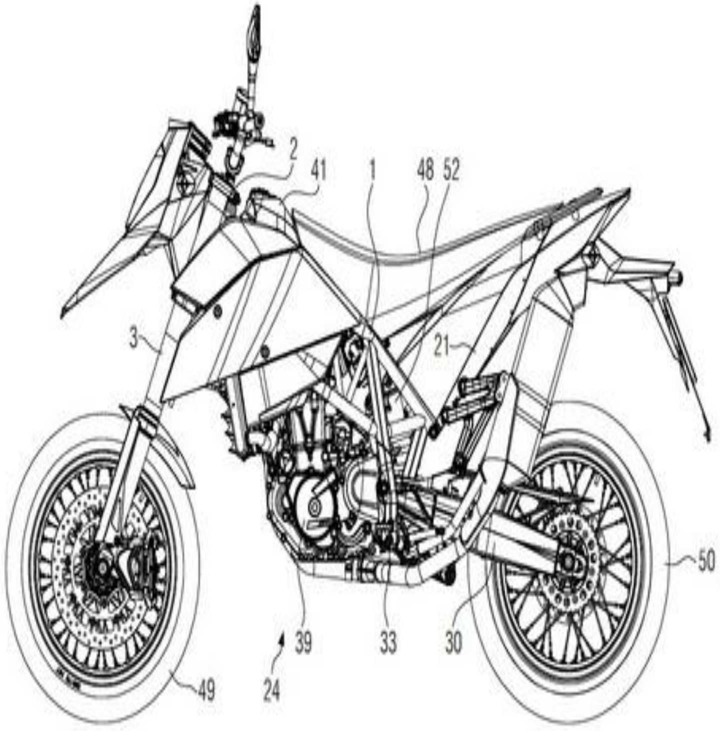
- **Intellectual Property Right (IPR)** means **the legal right of a person to own and protect their ideas or creations**, like books, drawings, songs, computer programs, logos, and inventions, so that **others cannot copy or use them without permission**.
- IPR protects creations like books, music, software, logos, and inventions.
- It gives legal rights to the original creator or owner.
- It prevents others from copying or using work without permission.
- It encourages creativity, innovation, and fair competition.
- Some intellectual property rights are
  - Copyright , Trademark, Patent Right

Copyright

- Copyright is a legal right that protects original creative works.
- It means others cannot copy or use your work without your permission.
- What can be copyrighted: Books, notes, music, videos, photos, software, and artworks.
- A song made by a singer is protected by copyright; others can't upload it without permission.
- It protects creators from theft and gives them credit and benefit for their work.
- If someone violates copyright law, they can face **fines from NPR 10,000 to NPR 100,000 or jail up to 6 months** for the first offense — and higher penalties if repeated (higher fines or up to 1 year jail)

Patent

- A patent is a legal right given to an inventor to protect a new invention.
- It means **only the inventor can make, use, or sell the invention** for a certain time.
- New and useful machines, products, processes, or technologies.
- A new type of water purifier or a medical device invented by someone.
- In Nepal, a patent is valid for **7 years from registration** and can be renewed **two times for 7 years each (total up to 21 years)**.
- In many countries, patents usually last **about 20 years from the filing date** (subject to rules and fees).



Trademark

- A trademark is a sign (name, logo, symbol) that identifies and distinguishes a product or service.
- It helps customers know which brand a product comes from and prevents others from copying it.
- Brand names, logos, slogans, symbols and unique designs for products or services.
- A company’s logo (like the symbol on shoes or drinks) that makes it different from others.
- In **Nepal**, a registered trademark is valid for **7 years** and can be **renewed again and again for further 7-year periods**.
- Using someone’s registered trademark without permission can lead to **fines up to around NPR 100,000 and confiscation of goods** under Nepal’s law.

IT Policy 2072

- The IT Policy 2072 aims to use information and communication technology (ICT) to develop Nepal into a knowledge-based society.
- It focuses on improving digital literacy so more people can use computers and the internet effectively.
- The policy promotes e-governance, meaning many government services should be available online for easier access.
- It supports ICT infrastructure growth, like expanding broadband and internet access across the country.
- It encourages innovation, research, and IT industries to create jobs and boost the economy.

IT Policy

- **Core Vision & Mission**
- **Vision:** To transform Nepal into an information and knowledge-based society and economy.
- **Mission:** To make ICT a primary driver for sustainable development and poverty reduction

IT Policy

- **Key Goals (Targets by 2020)**
- The policy set ambitious benchmarks for the year 2020:
- **Internet Access:** Ensure 100% of the population has access to the internet.
- **Digital Literacy:** Reach at least 75% digital literacy among the population.
- **E-Government:** Provide 80% of government services online.
- **Broadband:** Ensure 90% of the population is covered by broadband services.

Assignments

- What is a digital society? Explain two positive and two negative impacts of digital society.
- Define computer ethics. Write any four ethical rules to follow while using computers and the internet.
- What is information security? Explain the CIA triad (Confidentiality, Integrity, Availability).
- Write any four objectives of information security.
- Define cybercrime. List any four examples of cybercrime.
- Differentiate between cybercrime and traditional crime. Write any two points.
- What is malicious software (malware)? Name any four types.
- Explain any one type of malware with an example.
- What is spam? Write any three problems caused by spam messages/emails.
- Write any five methods to protect yourself from cybercrime.
- Why is cyber safety important for students? Write any three reasons.
- What is Intellectual Property Right (IPR)? Name any three types of IPR.
- What is a digital signature? Write two advantages of digital signature.
- What is cyber law? Mention any two provisions of Cyber Law in Nepal (Electronic Transaction Act, 2063).
- What is ICT Policy in Nepal? Write any three objectives or importance of ICT Policy.