Ethics

Lecture 1

Define ethics:

- Ethical behavior conforms to generally accepted social norms

- Ethics refer to rules provided by an external source

- Ethics refers to the shared beliefs about right and wrong behavior within a society.

Morality and social norms:

Morality refers to the widely shared beliefs about right and wrong that form a consensus within a society. However, individual morals views can vary based on factors like culture, custom, conscience and life experiences

Virtues & Vices

Virtues are habits that encourage acceptable behavior

Vices are habits associated with unacceptable behavior.

Ethical Dilemmas

New situations may arise that existing rules do not address, requiring individuals to apply or create new rules. Ethical dilemmas often involve choices between competing rights or principles.

The importance of integrity

- Integrity is a cornerstone of ethical behavior.

- People with integrity:

- Act in accordance with a **personal code** of principles
- Extend to all people the **same respect** and consideration that you desire

- **Apply the same moral standards in all situations**

Ethics, Morals and laws

Ethics: Ethics refer to the **standards or codes of behavior** expected of an individual by a group, such as a **nation**, **organization**

Morals: Morals are personal beliefs about **right and wrong**. They are shaped by individual factors like **culture**, **religion**, and **life experiences**

Laws: Laws are a **system of rules** that govern our actions and are enforced by institutions like the police, courts, and law-making bodies.

(Ethics in the business world)

Increased likelihood of unethical behavior

-Globalization, economic pressures, and heightened awareness of violations have contributed to the increased likelihood of unethical behavior in business.

Consequences of unethical behavior

Unethical behavior has led to severe consequences for business, including financial losses, law suits, and damage to reputation

Example: The Enron Scandal

The collapse of Enron due to accounting fraud and the concealment of debts and losses is a classic example of the risks associated with unethical decision-making

Why fostering good business ethics is important? (5 Reasons)

- **Earning** the **trust** of the community
- **Building** an organization that runs **smoothly**
- **Fostering** good business **practices**
- **Preventing** bad publicity
- **Protecting** the organization and its employees from legal action

Fostering good business ethics:

Organizations can protect their brand and maintain public trust

Fostering good business ethics/Building customer loyalty

- Technology companies are focusing on attracting and retaining customer loyalty.

- **Carol Cone, head of Cone:**

the role of **Philanthropy** in showing company values through actions

- **Philanthropy** helps create a positive image for stakeholders

Ethical behavior in IT:

- **Privacy and data security:**

Its professionals must prioritize the protection of personal information and ensure the secure handling of sensitive data

- **Responsible use of technology:**

Its professionals should promote the ethical and appropriate use of technology, avoiding misuse of exploitation

- **Transparency and accountability:**

Its professionals should maintain transparency in their actions and be accountable for the impact of their work on individuals and society

- **Social Responsibility in action**

Such as: -

- Donating to **charities** and **nonprofits**
- Offering better employee **benefits**
- Funding initiatives that benefit society, even if not immediately

Lecture 2

Fostering good business practices

Good ethics can lead to positive business outcomes and improved profits. Companies that prioritize safety, quality and customer service can avoid costly issues. Strong employee relations can reduce turnover and boost morals. conversely, unethical behavior can result in negative consequences like lawsuits, lost sale, and damage to reputation, as seen in the cases of Dell and Enron.

Fostering good business practices

- **Positive outcomes:**

Good ethics can lead to improved profits, customer satisfaction, and employee relations.

- **Negative outcomes**

unethical behavior can result in lawsuits, lost sale and reputational damage

The Role of the ethics officer

Appointing a corporate officer provides leadership and vision in the area of business conduct.

- **Responsibilities:**

Ensures ethical procedures are implemented, maintains ethical culture, serves as ethics contact.

- **Importance:**

Sends a clear message about the importance of ethics, but ongoing effort is required

- **Background:**

Ethics officers come from diverse background like legal, HR, finance, auditing, security or operations

Ethical standards set by the board

The board of directors is responsible for overseeing the careful and responsible management of an organization. board members are expected to conduct themselves with the highest standards of personal and professional integrity, setting the example for companywide ethical conduct. Unfortunately, many employees still fear retaliation for believe reporting misconduct will note lead to action.

Ethical standards set by the board:

Board Oversight:

The board is responsible for overseeing the organizations' management and activities

Ethical Leadership:

Board members must set the standards of ethical conduct and create an environment where employees feel comfortable reporting issues

Reporting Challenge

Many employees are hesitant to report misconduct due to fear of retaliation or a belief that it won't lead to action

Ethical establishing a code of ethics

A code of ethics outlines an organization's key ethical concerns, values, and principles that guide decision-making. The code applies to all employees and focuses on ethical risks, offering guidance for recognizing and addressing issues, and providing mechanisms for reporting misconduct

For the code to be effective, it must be developed with employee input, fully approved by leadership, and consistently applied

Ethical establishing a code of ethics

Purpose:

outlines ethical concerns, values, principles to guide decision-making.

Scope:

Applies to directors, officers and employees, focusing on ethical risks in their roles

Effectiveness:

Requires employee input, leaderships [approval, and consistent application

Social audits and ethical practices

Audition practices

Organizations review their policies and practices to evaluate progress on ethical and social responsibility goals

Stakeholder engagement

The results of social audits are shared with stakeholders to organization's ethical and socially responsible behavior

Ethics training

organizations must actively promote and communicate their code ethics through comprehensive ethics education programs. these programs often involve Workshops where employees apply the code to realistic case studies and sharing examples of recent ethical decisions.

effective training the organizing's commitment to ethical conduct and can mitigate legal liability

Ethical criteria in employee appraisals

Fair treatment:

Employees should treat others fairly and respectfully

Multicultural competence:

Employees should demonstrate effectiveness in a multicultural environment

Personal accountability:

Employees should take responsibility for their actions and decisions

Continuous development:

Employees should strive to continuously improve themselves and develop others

Open communication:

Employees should communicate openly and honestly with stakeholders

Creating an ethical work environment

Reporting channels

Employees should have multiple avenues to report suspected unethical practices, with assurances of protection from retaliation

Ethical culture

Organizations without a strong ethical culture and leadership may inadvertently encourage unethical behavior

Ethical decision-making in the digital age

As technology continues to rapidly evolve, the need for ethical decision-making has become increasingly crucial. This overview explores the key steps the decision-making process and highlights the various philosophical approaches that can guide us in navigating the complex ethical challenges presented by information technology

Decision-making process:

Develop problem statement:

Gather and analyze facts - make no assumptions - identify stakeholders affected by the decision

Identify alternatives

Involve others, including stakeholders, in brainstorming

Evaluate and choose alternatives

What is the impact on you, your organization and other stakeholders - Evaluate alternative based on multiple criteria

Implement decision

Develop and execute implementation plan - provide leadership to overcome resistance to change

Evaluate results

Evaluate results against selected success criteria - were there any unintended consequences

Success

Decision-making process

Develop Problem Statement

A clear and concise problem statement is essential for effective decision-making, addressing the observed problem, affected parties, frequency, and severity.

Identify Alternatives

Collaborating with stakeholders can help identify various alternative solutions, while avoiding criticism during brainstorming to maintain a free flow of ideas.

Evaluate and Choose

Evaluate alternatives based on criteria like effectiveness, risk, cost, and time, considering applicable laws, guidelines, and principles to select an ethically and legally defensible solution.

Implement Decision

Efficient and effective implementation is crucial, requiring clear communication and a transition plan to help stakeholders adapt to the change.

Evaluate Results

Monitoring outcomes, assessing whether goals were achieved, and examining unintended consequences can reveal the need for adjustments to the solution.

Ethical decision-making frameworks:

Virtue Ethics

Focuses on how one should behave and think about relationships within a community, suggesting that people's virtues guide them toward "right" decisions. However, the definition of virtue can be subjective and context-dependent.

Utilitarian Approach

Emphasizes choosing actions or policies that produce the greatest overall benefits for all affected individuals, but it can be challenging to measure and compare the values of certain benefits and costs.

Fairness Approach

Focuses on equitable distribution of benefits and burdens, but personal bias can influence decisions, and some groups may perceive policies as unfair.

Common Good Approach

Views society as people working together toward shared goals and values. Decisions based on this idea aim to create systems and services that benefit everyone, like quality education, safe transportation, and accessible healthcare. However, a challenge is that people may disagree on what the common good means.

Ethical decision- making approaches:

1- Virtues Ethics:

- Focus on character

- Emphasizes moral habits

- Subjective virtues

2- Utilitarian approach:

- Maximizes overall benefits

- Balances interests

- Hard to measure outcomes

3- Fairness

- Equal treatment

- Equitable distribution

- Influenced by bias

4- Common good

- Collective benefit

- Shared goals

- Varied interpretations

Ethical Challenges in Information Technology

Employee Monitoring

Balancing the need to protect company resources and ensure productivity with respecting employees' privacy and autonomy.

Copyright Violation

Illegal downloading of copyrighted content, causing significant financial losses to creators and copyright holders.

Spam Marketing

Unsolicited emails used for low-cost marketing, raising concerns about privacy and the ethical boundaries of direct marketing.

Data Breaches and Identity Theft

Hackers infiltrating databases to steal customer information, leading to fraudulent accounts and purchases.

Plagiarism in Education

Students downloading and plagiarizing content from the internet, compromising the integrity of their education.

Online Tracking

Websites planting cookies or spyware to track visitors' online behavior and purchasing habits, raising privacy concerns.

Lecture 3

IT Professionals: Roles, Responsibilities, and Relationships

IT professionals play a crucial role in modern society, requiring specialized knowledge and skills. This presentation explores the definition of professionals, the status of IT workers, and the various relationships they navigate in their careers. We'll examine the evolving professional services industry and the ethical considerations IT workers face in their interactions with employers, clients, suppliers, colleagues, users, and society at large.

IT Professionals

IT professionals require specialized knowledge and extensive academic preparation. According to U.S. regulations, a professional must meet four criteria: advanced knowledge in a field of science or learning, original and creative work, regular application of discretion and judgment, and primarily intellectual work that cannot be standardized. While IT workers often meet these criteria, they are not legally recognized as professionals due to lack of licensing.

IT Professionals

Advanced Knowledge

Acquired through prolonged study in a specialized field

Creative Work

Original and inventive in nature

Discretion and Judgment

Regular application in decision-making

Intellectual Work

Varied and non-standardized results

The Evolving Professional Services Industry

The professional services industry, including IT, is undergoing significant changes driven by seven key forces identified by Ross Dawson: client sophistication, governance, connectivity, transparency, modularization, globalization, and commoditization.

These forces are reshaping how IT professionals interact with clients and deliver services in an increasingly competitive and interconnected global market.

Evolving professionals' services industry

1- Modularization

- Take breakdown

- Internal Vs outsources

2- Globalization

- Global market

- Competitive landscape

3- Governance

- Scandals

- Stricter rules

4- Connectivity

- Easy communication

- Fast Access

5- Client sophistication

- Informed clients

- Quality services

6- Transparency

- Project progress

- Client feedback

7- Commoditization

- Cost-effective solutions

- Collaborative partnerships

The Evolving Professional Services Industry

Client Sophistication

Informed and Demanding Clients: Clients are knowledgeable about their needs, seek quality services, and expect favorable terms.

Governance

Increased Oversight and Trust Issues: Scandals and stricter rules have decreased trust and increased oversight in client-service provider relationships.

Connectivity

Global Communication and Instant Access: Clients and service providers rely on easy and fast worldwide communication through technology.

1) Transparency

Real-time Updates and Feedback: Clients want to see project progress, provide feedback, and influence the project's direction.

2) Modularization

Flexible Outsourcing: Clients can break down tasks and decide which to do them internally and which to outsource.

3) Globalization

Global Competition: Clients can choose service providers from anywhere in the world, creating a competitive market.

4) Commoditization

Price-Driven Services and Partnerships:

Clients prioritize cost-effective solutions for basic services but seek collaborative partnerships with service providers for more complex services.

Professional Relationships That Must Be Managed:

IT professionals are involved in various relationships with:

- ✓ Employers
- ✓ Clients
- ✓ Suppliers
- ✓ Colleagues
- ✓ Users of IT systems
- ✓ Society

In each of these interactions, ethical IT professionals act with honesty and integrity.

Professional IT Workers and Employers

Complex Agreements: IT workers and employers must establish clear agreements regarding job responsibilities, performance expectations, and company policies.

Ethical Conduct:

IT professionals are expected to set a positive example in ethical IT usage and protect company resources.

Key Ethical Issues:

Software piracy, trade secrets, and whistleblowing are significant ethical concerns in the IT industry.

BSA Anti-Piracy Efforts:

The Business Software Alliance (BSA) actively combats software piracy and imposes severe penalties on violators.

IT Workers and Clients

IT workers often provide services to external or internal clients, exchanging value through contracts. Successful collaboration requires mutual trust and shared decision-making responsibilities.

Ethical issues can arise when IT consultants recommend their own products or when project status reports are inaccurate. Legal disputes may involve allegations of fraud, misrepresentation, or breach of contract.

IT Workers and Clients

1) Agreement

IT workers and clients exchange value through contracts outlining responsibilities and terms.

2) Collaboration

Successful partnerships require shared decision-making and trust between parties.

3) Challenges

Ethical issues may arise from conflicts of interest or inaccurate project reporting.

IT Project Challenges

1) Scope Changes

Client-initiated alterations to project requirements can cause issues.

2) Poor Communication

Misunderstandings between client and vendor may lead to lead to unmet expectations.

3) Undisclosed Information

The client didn't talk about legacy systems that complicate the complicate the new system’s implementation.

Relationships Between IT Workers and Suppliers

Building strong relationships with suppliers:

- IT workers deal with many suppliers for hardware, software, and services.
- Good relationships help with communication and sharing ideas.
- Teamwork can lead to creative and cost-effective solutions.
- Treat suppliers fairly and avoid unreasonable demands.

Relationships Between IT Workers and Suppliers

Avoiding unethical behavior:

▪ Suppliers want to maintain good relationships with customers,

Some suppliers might offer bribes.

▪ IT workers should be careful and avoid accepting bribes,

Even small things like gifts or invitations can be considered bribes.

Relationships Between IT Workers and Suppliers

Understanding bribery:

• Bribery is giving something of value to someone in business or government to gain an advantage, A common example is a kickback.

• Both the giver and the receiver can face legal problems.

• Bribery can void contracts but rarely leads to criminal charges.

Relationships Between IT Workers and Suppliers

1-Giving gifts in business:

• In some cultures, gifts are important for business.

• In the U.S., gifts like sports tickets might be offered.

• It's important to know when a gift becomes a bribe.

2-Transparency is key:

- Gifts should always be open and declared.
- Undeclared gifts can be seen as bribes.
- Companies often have rules about reporting and declining gifts.
- Some companies donate gifts to charity.

Bribes Vs Gifts

1)

Bribes: Are made in secret, as they are neither legally nor normally acceptable

Gifts: Are made openly and publicly, as a gesture pf friendship or goodwill

2)

Bribes: Are often made indirectly through a third party

Gifts: Are made directly from donor to recipient

3)

Bribes: Encourage an obligation for the recipient to act favorably toward the donor

Gifts: Come with no expectations of a future favor for the donor

Relationships Between IT Workers and Other Professionals

Professional Loyalty and Ethics:

- **Loyalty among peers:** Professionals often support each other in finding jobs but may be hesitant to criticize publicly.
- **Reputation of the profession:** Professionals care about how their profession is perceived, as it affects individual members.
- **Ethical standards:** Professionals are responsible for upholding ethical standards and codes of conduct.
- **Mentorship:** Experienced professionals can guide and develop new members.

Relationships Between IT Workers and IT Users

- **IT users:** Individuals who use IT products.
- **IT workers:** Develop, install, maintain, and support IT products.
- **IT workers' responsibilities:** Understand user needs, deliver effective solutions, and promote ethical behavior among users.

Relationships Between IT Workers and Society

- **Regulatory laws:** Set safety standards but may not be comprehensive.
- **Professional responsibility:** IT professionals should understand potential impacts of their work and take preventative measures.
- **Societal expectations:** IT professionals should contribute positively and avoid causing harm.
- **Professional standards:** Guide IT professionals in maintaining ethical standards.

Key Points

❖ IT workers play a crucial role in both organizational and societal contexts.

❖ They have a responsibility to understand and meet the needs of IT users while ensuring ethical behavior.

❖ Their work can have significant impacts on society, and they should take steps to mitigate risks.

❖ Professional organizations offer codes of ethics to guide IT professionals in their work.

Lecture 4

Components of professional codes of ethics

- ### Aspirational Component
  Express the organization's **ideals** and **goals**
- ### Regulatory Component
  Lists **rules** and **principles** members are expected to follow

Many code of ethics emphasizes the importance of ongoing learning **(Continuous Education)** in the field.

Benefits of adhering to professional codes of ethics

1- Ethical Decision Making
Ensures practitioners use share core values and beliefs when facing ethical dilemmas

2- High Standards of practice
Serves as reminder of responsibilities and duties, even under business pressures

3- Public trust and respect
Strengthens public confidence in professionals and enhances respect for individuals and the profession

4- Evaluation benchmark
Provides a standard for self-assessment and peer evaluation

Roles of professional organizations in IT

- Professional organizations play a **crucial role** in the **rapidly evolving IT field**.
- They provide **platforms** for **networking**, **idea exchange**, and **continuous skill enhancement**.
- These organizations **disseminate** information through various channels, including email, periodicals, websites, meetings, and conferences.
- Many have developed codes of ethics, recognizing the need for professional standards of competence and conduct.

A List of five leading professional organizations in the field of information technology is presented below.

- ✓ **A**ssociation for **C**omputing **M**achinery (ACM)
- ✓ **A**ssociation of **I**nformation **T**echnology **P**rofessionals (AITP)
- ✓ **I**nstitute of **E**lectrical and **E**lectronic **E**ngineers **C**omputer **S**ociety (IEEE-CS)
- ✓ **P**roject **M**anagement **I**nstitute (PMI)
- ✓ **S**ys Admin, **A**udit, **N**etwork, **S**ecurity (SANS) Institute

ACM

- **Founded in 1947**
- Is a global computing society with over **92,000 members** across **100+ countries**
- It **Offers** numerous publications and electronic forums for technology workers, including **Tech news, Career News, RISKS Forum, Queue casts, eLearn, and ubiquity**
- Also provides a substantial digital library and sponsors 34 special-interests groups (SIGs) in major computing areas
- Has a code of ethics and professional conduct with supplemental explanations and guidelines

The ACM Code Consists Of:

- Eight general moral imperatives
- Eight specific professional responsibilities
- Six organizational leadership imperatives
- Two elements of compliance

AITP

- One of the **oldest** IT associations.
- It offers various professional development programs, including the **Information Systems Analyst (ISA)** Certification.
- Provides networking opportunities through local branches and national conferences.
- It's code of ethics emphasizes integrity, competence, professional development, and advancing IT knowledge

IEEE-CS

- **Founded in 1946**
- Is one of the **oldest** and **largest** IT professional associations with approximately **85,000** members
- It offers technical journals, magazines, conferences, books and online courses.
- This society provides certification programs like **CSDP** and **CSDA**, and sponsors numerous conferences and research-focused journals.

The IEEE-CS and ACM created a committee in 1993 to establish software engineering as a profession. This committee suggested setting ethical standards, defining essential knowledge and practices, and outlining educational programs for software engineers.

PMI

- **Founded in 1969**
- Has grown to over **420,000** members and certified individual in more than **170 countries.**
- Its membership includes project managers from various fields, including construction, sales, finance, production, and information systems.
- Offers education, certification, and networking opportunities, with widely recognized certifications like the project management professional **(PMP)** Credential.

SANS

- Provides comprehensive information security training and certification programs.

- It trains approximately **12,000** individuals annually, with over **165,000** security professionals worldwide having participated in its course.

- SANS publishes weekly news (News Bites) and security vulnerability summaries, and offers timely security alerts.

- Maintains a collection of over 1,200 research documents on various information security topics and operates the **Internet Storm Center**.

- The **Internet Storm Center (ISC)** is a program by the SANS Technology Institute that monitors and reports on **malicious activity online**. It provides analyses, insights, and resources related to **cybersecurity threats**.

IT Certification and licensing

- In the world of Information Technology, **certification** and **licensing** play crucial roles in validating professional skills and knowledge.
- While **certification** is generally voluntary and can apply to both **individuals** and **products**,
- **licensing** is mandated by law and exclusively for individuals.
- This presentation explores the various aspects of IT certification, including vendor-specific programs, industry association certifications, and government licensing requirements.

What is certification

- **Certification** is a process that verifies a professional's specific set of skills, knowledge, or abilities, as determined by the certifying organization.
- Unlike **licensing**, **certification** is typically voluntary and can be applied to both individuals and products.
- For example, the **Wi-Fi CERTIFIED** logo ensures product compliance with interoperability standards.
- **IT-related certifications** may or may not require adherence to a code of ethics, which is more common in licensing.
- The value of certifications is debated, with some employers viewing them as indicators of fundamental knowledge, while critics argue they cannot replace practical experience

PROS & CONS OF CERTIFICATION

Pros

- Demonstrates mastery of knowledge
- Provides structured learning
- Aligns with career development

Cons

- May not replace experience
- Skepticism from some employers
- Potential revenue focus for vendors

Vendor Certification

- Many IT vendors, including Cisco, IBM, Microsoft, Sun, SAP, and Oracle, offer certification programs for their products.
- These certifications allow professionals to identify themselves as certified users of specific technologies. Depending on market conditions, certain certifications can significantly enhance an IT worker's salary and career prospects.

Vendor Certification

- **Vendor certifications** are particularly relevant for job roles with highly specific requirements. However, they may sometimes focus too heavily on technical details of the vendor's technology, neglecting more general concepts.
- Most **certifications** use multiple-choice exams due to legal concerns with other grading methods. Some, like the CCIE, also need practical lab exams. Gaining the experience for these certifications can take a long time.

Vendor Certification

1- Examination

Pass a written exam, typically in multiple-choice format

2- Hands-on Testing

Some certifications, like CCIE, require practical lab exams

3- Experience

Acquire necessary experience, which can take years

4- Preparation

Study materials and training courses available at varying costs

Lecture 5

Preparing for IT Certifications:

1- Study Materials

Comprehensive books and guides to prepare for certification exams

2- Online Courses

Interactive online training programs for certification preparation

3- Practical Labs

Hands-on experience crucial for certain certifications like CCIE

Industry Association Certification

- Various industry certifications exist in different IT-related subject areas. Their value can vary depending on an individual's career stage, existing certifications, and the specific IT job market. For example, a 2007 study showed that certified security professionals generally receive at least a 10% higher salary compared to non-**certified** individuals.

- These certifications typically require prerequisite **education** and **experience**, **passing** an exam, and **adhering** to a code of ethics. Maintenance often involves annual fees, continuing education credits, and sometimes renewal exams.

Industry Association Certifications

1- Broader Perspective

Industry association certifications often demand a higher level of experience and a wider perspective than vendor certifications.

2- Emerging Technologies

Associations may lag in developing tests for the latest technologies.

3- Holistic Approach

Combining technical, business, and behavioral competencies in certifications.

Project Management Certifications

- Given the ongoing demand for skilled project managers, the Project Management Institute (PMI) offers some of the most recognized and sought-after certifications. PMI provides certifications at various levels, with over 300,000 individuals worldwide holding some form of PMI certification.

- Obtaining PMI certification requires meeting specific education and experience requirements, agreeing to the PMI Code of Ethics, and passing the appropriate exam.

- College business majors are encouraged to acquire PMI's Certified Associate of Project Management before graduation to enhance future employment prospects.

Project Management Certifications

- **Certification Levels**
  PMI offers multiple certification levels to suit different career stages.
- **Education**
  Specific educational requirements must be met for each certification level.
- **Experience**

Relevant project management experience is required for certification.

- **Examination**

Candidates must pass the appropriate PMI exam for their desired certification.

Government Licensing in IT

In the U.S., a government license is an official approval that allows individuals to engage in specific activities or run a business, typically managed at the state level. The licensing process often includes passing an exam. Professions like certified public accountants (CPAs), lawyers, doctors, and certain engineers must be licensed to practice.

Government Licensing in IT

- ✓ States establish licensing laws to protect public safety.
- ✓ Texas created the Engineering Registration Act after a school explosion in 1937.
- ✓ Only licensed engineers can provide services to the public.
- ✓ All public projects must be supervised by a licensed engineer.
- ✓ Individuals must have a valid license to call themselves engineers and can face legal penalties for violations.

Government Licensing in IT

1. Legal Requirements
2. Only licensed individuals can provide engineering services to the public in many states.
3. Public Works
4. All public works must be designed and constructed under the supervision of a licensed professional engineer.
5. Title Protection
6. Individuals may not refer to themselves as engineers or professional engineers without a valid license.
7. Penalties
8. Legal consequences exist for those who violate licensing regulations.

Certification vs. Licensing

- **Certification and licensing** validate professional competence.
- **Certification** is generally voluntary and can apply to both individuals and products.
- **Licensing** is mandated by law and exclusively for individuals.

Certification vs. Licensing

Aspect	Certification	Licensing
Mandatory	Generally voluntary	Required by law
Applies to	Individuals and products	Individuals only
Issued by	Private organizations, vendors	Government entitles
Code of ethics	May or may not be required	Typically required

The Value of IT Certifications

- Knowledge Validation
- Career Advancement
- Structured Learning
- Industry Recognition

The Future of IT Certification and Licensing

- Industry groups are creating certifications for wider roles, like project management and network security.
- As technology spreads across industries, IT certification and licensing will become more *important to keep professionals skilled and ethical*.

Importance of IT in Modern Systems:

- **Enterprise Resource Planning:**
  manage all aspects of their operations, including forecasting, production planning, purchasing, inventory management, manufacturing, and distribution.
- **Critical Infrastructure:**
  computer and information systems oversee nuclear reactors in power plants.
- **Government Operations:**
  Government information systems are digital platforms and databases designed to manage and distribute critical services and resources as Tax System, Medicare Information Systems.

Arguments for Licensing IT Professionals

1- Professional Standards:

Promote adherence to high professional standards among IT workers.

2- Ethical Conduct:

Encourage IT professionals to follow a code of ethics.

3- Accountability:

Establish consequences for violations, addressing the current lack of accountability in the field.

4- Malpractice Standards: Without licensing, there are no clear standards to handle professional mistakes in IT.

Challenges in Implementing IT Licensing

- **Skill Standardization**

  No universal agreement on essential skills and knowledge for licensed IT professionals.

- **License Validity**

  Uncertainty about whether a license is recognized across different regions or countries.

- **Exam Administration**

  Issues around who designs and manages licensing exams.

- **Rapid Technological Change**

  Licenses may need frequent updates as technology changes quickly.

The Professional Malpractice

IT professional malpractice occurs when an IT professional fails to perform their duties competently, causing harm or loss to a client or user. This can result from mistakes in software development, poor data management, security issues, or inadequate support, where the professional does not meet the expected standard of care for their role.

The Professional Malpractice

Issue	Challenge
Lack of uniform standards	No consistent benchmarks for evaluating professional conduct
Absence of licensing	Difficult to prove professional negligence
Court Precedent	Consistent rejection of computer-related malpractice suits
Professional Accountability	Challenging to hold software engineers accountable through malpractice lawsuits

Common Ethical Issues for IT Users

- **Software Piracy**

unauthorized use of legally protected software, which includes stealing, copying, distributing, modifying or selling the software.

- **Misuse of Computing Resources**

Employees visiting non-work-related websites, participating in chat rooms, viewing restricted, or playing games during work hours.

These activities reduce productivity and waste company time.

- **Inappropriate Sharing of Information**

Unauthorized sharing of sensitive private or confidential information, violating privacy rights and potentially exposing the company to competitive risks and threats.

For example, salaries and health records and business plans

Supporting Ethical IT Practices

As IT use grows, so does the risk of unethical behavior. Many organizations create policies to prevent misuse. While no policy can stop all unethical actions, it can clarify the rights and responsibilities of IT users and outline acceptable behavior. Following these policies can improve services, increase productivity, and lower costs. Here are some steps to develop an IT usage policy:

1. Establish Software Guidelines

Create clear rules governing the use of home computers and associated software, ensuring employees have legal copies of necessary software.

2. Define Appropriate Use

Create, communicate, and enforce clear guidelines for using corporate IT resources to enhance job performance while allowing limited personal use.

3. Protect Data and Information

Implement systems that restrict data access to employees who need it for their roles, protecting sensitive information.

4. Maintain Corporate Firewall

Install and maintain a firewall to regulate access based on the company's internet usage policy, blocking inappropriate content and reducing security risks.

Lecture 6

Pillars of Professionalism

- Provide a framework of ethical standards and values that guide behavior in the computer profession, helping professionals navigate complex and dynamic challenges with integrity and respect.
- In computer and information technology fields, where professionals work with sensitive data, create impactful systems, and safeguard online communities, these four pillars—Commitment, Integrity, Responsibility, and Accountability—are essential to fostering trust and maintaining high standards of professionalism.

Pillars of Professionalism:

1- Commitment

2- Integrity

3- Responsibility

4- Accountability

1- Commitment

Commitment is characterized by willingness and dedication to fulfilling responsibilities. For true commitment:

- ✓ It must be made voluntary, without force, and ideally aligns with personal interest.
- ✓ Effort must be made to fulfill it, even if assistance is needed.
- ✓ Clear understanding of roles and tasks is essential, as well as a shared commitment among team members.
- ✓ Commitments should be made openly, with resources like time and materials specified.
- ✓ If it becomes clear that a commitment cannot be met, notifying relevant parties in advance and renegotiating demonstrates accountability and respect for others' expectations.

2- Integrity

Integrity means being true to one's beliefs, showing honesty, and upholding self-worth. It involves:

- ✓ **Vision**: planning ahead to avoid challenges and maximize benefits.
- ✓ **Passion**: excelling due to a genuine love for the work.
- ✓ **Commitment**: bonding to one’s work through vision and passion until tasks are completed.

3- Responsibility

Responsibility relates to the actions one must take and the consequences of those actions. It varies by role, such as:

- ✓ **Service Responsibilities:** Professionals must deliver services within set times, maintain quality, and ensure client safety.
- ✓ **Product Responsibilities:** In product-related roles, professionals must ensure product quality, provide user guidance, and handle liability issues.
- ✓ **Consequential Responsibilities:** Actions often have aftereffects, where successful outcomes bring praise, but failures can bring serious consequences, as in the example of a medical professional making a critical mistake during surgery.

4- Accountability

Accountability is the obligation to answer for fulfilling responsibilities. It involves:

- ✓ **Outcome Measures:** Reliable standards to assess performance, like student success rates in teaching.
- ✓ **Performance Standards:** Defined standards based on outcome measures, customized for each profession.
- ✓ **Incentives and Penalties:** Motivational rewards and consequences help maintain standards without encouraging dishonesty or fear of punishment.

IT Security Incidents: A Major Concern

The Importance of IT Security

I. **Growing Threats:** IT security incidents pose serious risks to business operations, financial stability, and reputation.

II. **Types of Incidents:** Data breaches, unauthorized access, malware, and system failures.

III. **Key Impact:** Compromise or loss of sensitive data and critical infrastructure.

Why IT Security is Crucial?

I. **Increased Risk:** As businesses depend more on digital infrastructure, the risk of cyber incidents is rising.

II. **Essential Actions:** Continuous vigilance and proactive security management to protect assets and reputation.

III. **Protecting Sensitive Information**

Confidential business, customer, and employee data must be safeguarded.IT systems need strong protection from theft, disruption, and other malicious activities.

IV. **Balancing Security with Business Needs**

Challenges:

Balancing high security with operational efficiency.
Managers, IT professionals, and IT users all face ethical dilemmas in IT security.

A range of ethical dilemmas pertaining to IT security:

Response to Cybercrime: Should the organization take legal action or handle the .I issue discreetly to avoid negative publicity? Should affected customers be notified or addressed differently?

Investment in Security: What level of investment is sufficient to protect against .II cybercrime? How secure is "secure enough"?

Addressing Software Vulnerabilities: If company software has vulnerabilities that risk .III unauthorized access, what corrective actions should be taken?

Balancing Security and Usability: How should the organization handle security .IV measures that inconvenience customers or employees, potentially reducing sales or increasing costs?

Why Are Computer Incidents So spread?

1- Increasing Complexity:

Modern computing depends on highly complex interconnected networks, devices, and systems.

Each additional device or network adds new entry points, raising the risk of breaches.

2- High User Expectations:

Users demand rapid issue resolution, pressuring support teams to skip identity checks.

Common shortcuts, like shared login credentials, can lead to unauthorized access.

3- Evolving Systems:

Shift from isolated systems to networked environments (e.g., e-commerce, mobile computing).

Growing reliance on interconnected technology heightens security demands and risks.

4- Dependence on Vulnerable Software:

Known software vulnerabilities can be exploited if not patched promptly.

Some organizations delay updates to avoid reducing software usability, increasing risk exposure.

Types of Exploits

❖ Cyberattacks are constantly evolving, targeting not only computers but also smartphones.

❖ Smartphones are now key targets as they store sensitive information and are used for online transactions.

❖ Experts warn that cyberattacks on smartphones may soon rise, aiming to steal data or control devices remotely.

Common Attack Types:

- **Viruses**
- **Worms**
- **Trojan Horses**
- **Botnets**
- **DDoS Attacks**
- **Rootkits**
- **Spam**
- **Phishing**

Virus

- Pieces of programming code
- Usually masked as something else as files or programs
- Cause unexpected and undesirable behavior
- Often attached to files
- Spread by actions of the “infected” computer user
- Infected e-mail document attachments
- Downloads of infected programs
- Visits to infected Websites

Worms

- Harmful programs
- Reside in active memory of a computer
- Duplicate themselves
- Can propagate without human intervention
- Negative impact of worm attack
- Lost data and programs
- Lost productivity
- Additional effort for IT workers

Trojan Horses

- Malicious code hidden inside seemingly harmless programs
- Users are tricked into installing them
- Delivered via email attachment, downloaded from a Web site, or contracted via a removable media device

Logic bomb:

Activates when triggered by specific events, such as:

1- A certain date or time - Running a specific program

2- Deleting a user account -Remains hidden until the trigger occurs.

Once activated, it executes malicious code, causing harm to the computer.

Botnets:

A botnet is a collection of computers (bots) that have been infected with malicious software and are controlled remotely by a hacker.

1- Unknown Control: Owners are usually unaware their devices are part of a botnet.

2- Main Uses: Botnets are used to distribute spam, launch attacks, or perform other malicious tasks, often without the knowledge of the computer owner.

3- Powerful Networks: Large botnets can be more powerful than even the most advanced supercomputers.

- **Nature Behavior:**

1- Virus:

- Requires Human Interaction
- Spreads Via Infected Files

2- Worm:

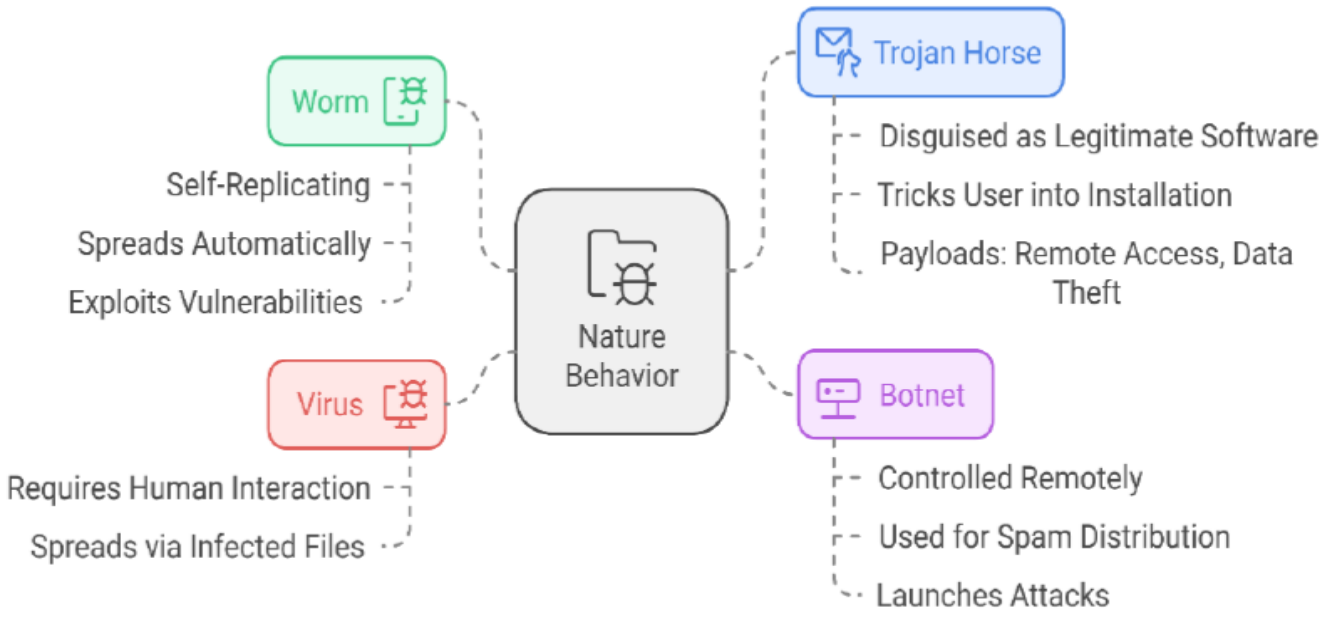
- Self-Replicating
- Spreads Automatically
- Exploits Vulnerabilities

3- Trojan Horse:

- Disguised as legitimate software
- Tricks User into Installation
- Payloads: Remote Access, Data Theft

4- Botnet:

- Controlled Remotely
- Used for spam Distribution
- Launches Attacks



Malware Types:

1- Virus:

- User Action Required
- Infected Files
- Executable Programs

2- Worm:

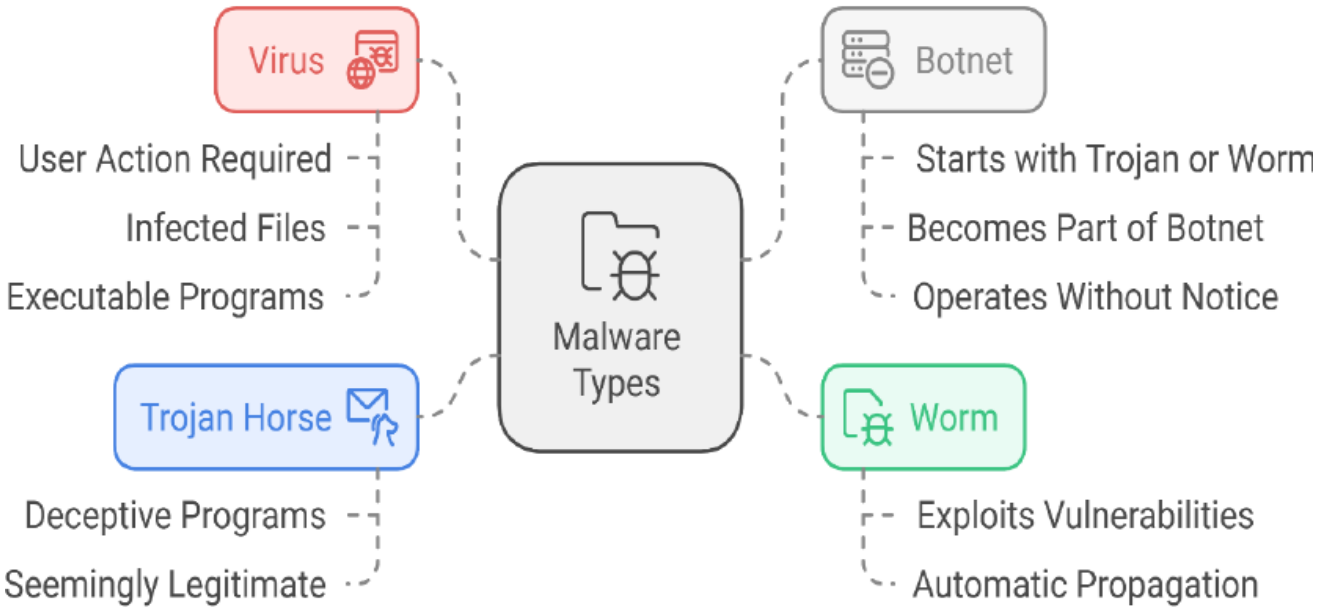
- Exploits Vulnerabilities
- Automatic Propagation

3- Trojan Horse:

- Deceptive Programs
- Seemingly Legitimate

4- Botnet:

- Starts with Trojan or Worm
- Becomes Part of Botnet
- Operates Without Notice



- **Malware Propagation Methods**

1- Virus:

- Executable Files
- Documents
- Programs
- User Interaction

2- Worm:

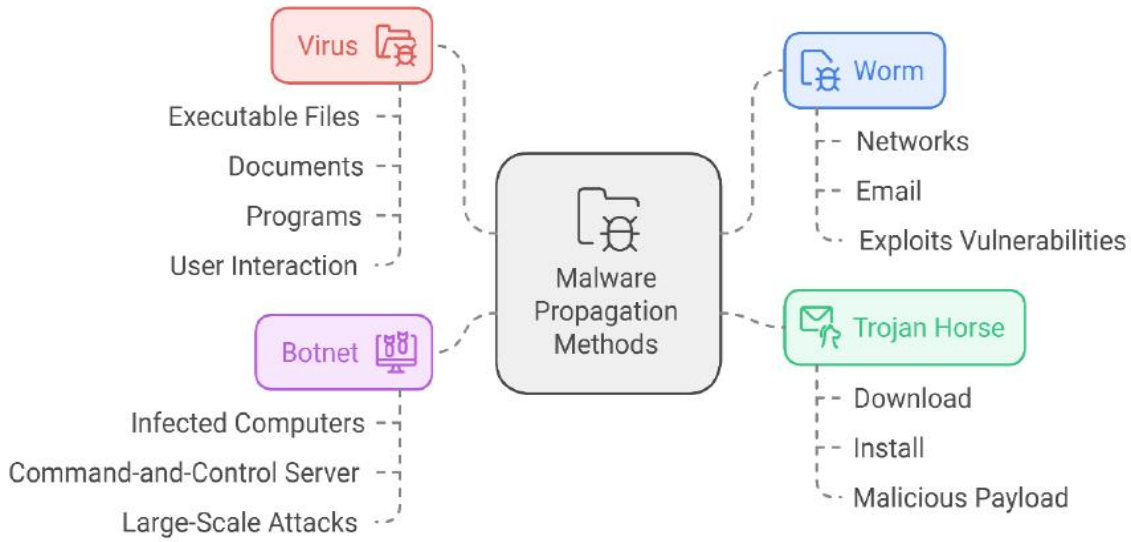
- Network
- Email
- Exploits Vulnerabilities

3- Trojan Horse:

- Download
- Install
- Malicious Payload

4- Botnet:

- Infected Computers
- Command-and-Control Server
- Large-Scale Attacks



- **Malicious Software Payloads**

1- Virus:

- Disruptive Messages
- Corrupting Files
- Deleting Data
- Reformatting Hard Drives

2- Worm:

- Consuming Bandwidth
- Crashing Systems
- Data Theft
- Installing Backdoors

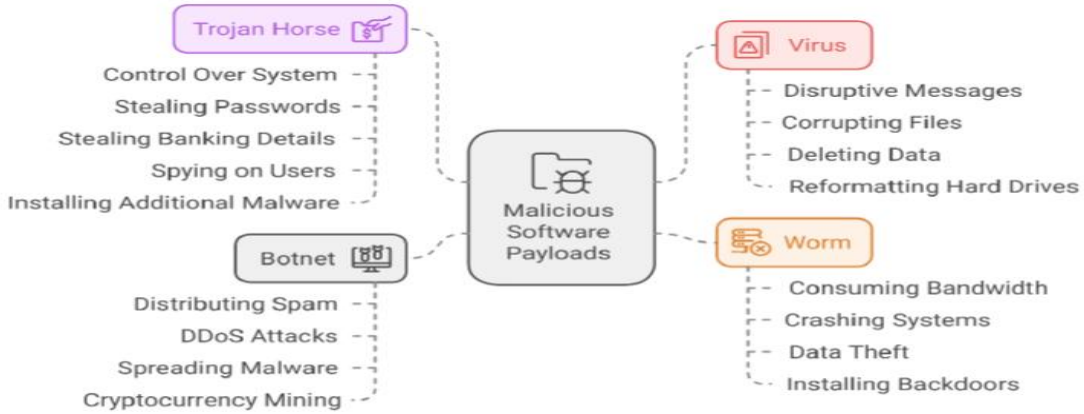
3- Trojan Horse:

- Control Over System
- Stealing Passwords
- Stealing Banking Details
- Spying on Users
- Installing Additional Malware

4- Botnet:

- Distributing Spam
- DDos Attacks
- Spreading Malware
- Cryptocurrency Mining

Malicious Intent (Payload):



- **Signs of Infection**

1- Virus:

- Slow System Performance
- Corrupted Files
- Unusual Messages
- Evade Detection

2- Worm:

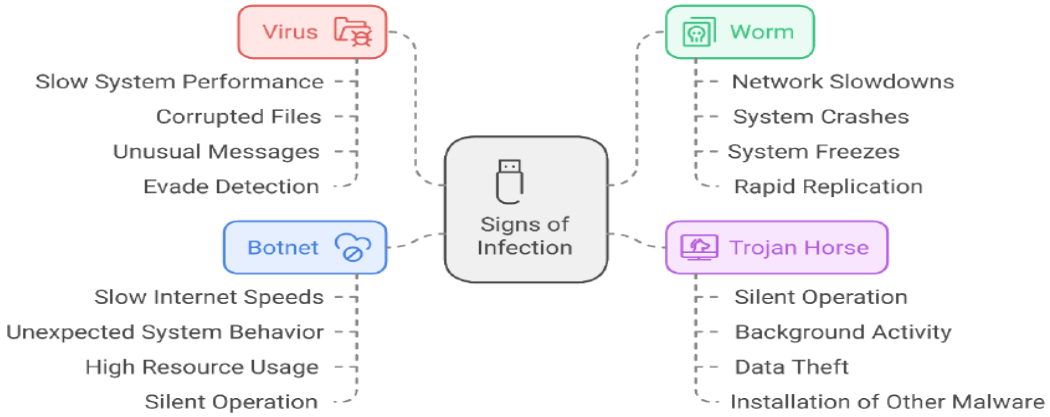
- Network Slowdowns
- System Crashes
- System Freezes
- Rapid Replication

3- Trojan Horse:

- Silent operation
- Background Activity
- Data Theft
- Installation of other Malware

4- Botnet:

- Slow internet Speeds
- Unexpected System Behavior
- High Resource Usage
- Silent Operation



Aspect	Virus	Worm	Trojan Horse	Botnet
Nature and Behavior	Malicious code attached to a file or program that requires human action to propagate.	Self-replicating program that spreads without user intervention.	Disguised as legitimate software; no self-replication.	Network of infected computers controlled remotely by a hacker.
Method of Propagation	Spreads via infected files, email attachments, or downloads; requires user interaction.	Spreads automatically across networks by exploiting vulnerabilities.	Relies on users to download and run the host program; spread through deception.	Spread by worms or Trojans; infected machines are remotely controlled.
Malicious Intent (Payload)	May corrupt files, display messages, or delete data.	Consumes network bandwidth, crashes systems, or installs backdoors.	Steals sensitive information, gains remote control, or installs more malware.	Performs large-scale tasks like spam distribution or DDoS attacks.
Detection and Signs of Infection	Slower system performance, corrupted files, or unusual messages.	Slower network performance, system crashes, or freezing.	Often silent; users may not notice until damage is done (e.g., stolen data).	Silent infection; may cause slow internet speeds or high resource usage.
Dependency on User Action	Requires user action (e.g., opening an infected file) to spread.	Spreads automatically without user interaction.	Depends on tricking users into running malicious software.	Initial infection requires Trojan or worm; operates without user knowledge.
Scope and Scale of Attack	Affects individual computers, spreads through file sharing or email.	Can infect entire networks rapidly, large-scale disruption.	Targets specific systems, often for data theft or remote control.	Affects thousands or millions of computers, used for coordinated attacks.

Distributed Denial-of-Service (DDoS) Attacks

A DDoS attack involves multiple compromised computers flooding a targeted website with requests, making it unavailable to real users.

- **Unlike other attacks,** DDoS doesn't breach the target system but overwhelms it with excessive requests, causing it to run out of resources.
- **Attackers** download small programs onto many computers worldwide.
- **These infected computers,** called "zombies," are activated to repeatedly send access requests to the target site.
- **Preventative Measures:** Restoring compromised systems often involves reinstalling trusted software backups and applying patches to prevent future attacks.

Rootkits

A set of software tools that give attackers unauthorized control of a system to gain administrator-level access.

- Allows **attackers** to execute files, view logs, monitor activities, and change system settings without detection.
- **Rootkits** consist of a **dropper** (installs rootkit), a **loader** (injects rootkit into memory), and the rootkit itself.
- **Dropper Activation:** Triggered by actions like clicking malicious links or opening infected files.
- **Loader Execution:** Injects the rootkit into the system, then self-deletes, leaving the rootkit hidden.

Rootkits

- ### Challenges and Detection

Rootkits are hard to detect due to their deep system integration.

- ### Signs of Infection:

- System freezes or slow responses.
- Screensaver or taskbar changes.
- Slowed network speeds.

- ### Remediation: Complete Reinstallation

Removing a rootkit often requires reformatting the disk, reinstalling the operating system and applications, and restoring user settings, which can be time-intensive and result in data loss.

Spam

Spam refers to the misuse of email systems to distribute unsolicited (unwanted) emails sent to a large number of recipients.

- **Commercial advertising:** Most spam is used for advertising products or services.
- **Legitimate business use:** Some businesses use spam for marketing purposes.

Why companies use of Spam in Businesses? :

- **Low cost:** Email marketing is cheaper than traditional methods like direct mail.
- **Quick turnaround:** Email campaigns can be created and distributed faster.

Rapid feedback: Email campaigns can provide quicker results.

Spam

What are the negative Impacts of Spam?

- **Cluttered inboxes:** Spam can make it difficult to find important emails.
- **Wasted time:** Users spend time deleting spam.
- **Increased costs:** Spam increases costs for internet service providers (ISPs) and online services. These increased costs can lead to higher subscription fees for all users.

Phishing

A type of fraud where attackers use deceptive emails to trick recipients into revealing personal information.

- Phishing is a trick where scammers (fraudulent) send fake emails to trick people into giving away their personal information, like passwords or credit card numbers. These emails often look real and try to scare people or promise big rewards to get them to act quickly.

Phishing

Phishing attacks often involve:

Deceptive emails: Scammers send fake emails that look real.

Malicious links or attachments: Clicking on these can lead to malware infections.

Fake websites: These websites are designed to steal personal information.

Phishing

➢ **Spear Phishing:** A Targeted Approach

Spear phishing is a more specific type of phishing attack

➢ **Targeted Emails:** Scammers send emails to specific individuals or organizations.

➢ **Impersonation:** They often pretend to be someone you know, like a boss or colleague.

➢ **Data theft:** The goal is to steal sensitive information, such as passwords and financial data.