SOCIAL & PROFESSIONAL ISSUES

I. ETHICS

Definition of Ethics

- It is the practical science of the morality of human actions
- It is the scientific inquiry into the principles of morality
- It is the science of human acts with reference to right and wrong
- It is the study of human conduct from the standpoint of morality
- It is the study of the rectitude of human conduct
- It is the investigation of life
- Ethics are beliefs regarding right and wrong behaviour

"Moral principles that govern a person's or group's behaviour."
"The branch of knowledge that deals with moral principles."

Terms Associated with Ethics

- **Science –** systematic study or a system of scientific conclusions clearly demonstrated, derived from clearly established principles and duly coordinated
- **Morality –** the quality of right or wrong in human acts
- **Human Acts –** acts done with knowledge and consent
- **Virtues –** habits that inclines us to do what is acceptable
- **Vices –** habits that inclines us to do what is unacceptable
- **Value System –** the complex scheme of moral values by which one chooses to live

Relationship of Ethics with other Science

1. Logic
2. Psychology
3. Sociology
4. Art
5. Politics
6. Education

Ethics and Logic

- Logic – the science of right thinking
- Ethics – the science of right living
- Both ethics and logic aim to rectitude: the former aims to at right doing; the latter, at the right thinking

Ethics and Psychology

- Psychology – studies how man behaves
- Ethics – studies how man ought to behave
- Both deal with the study of man, human nature, and human behaviour

Ethics and Sociological

- Sociology – includes the social order
- Ethics – deal with the moral order
- "Whatever does violence to the social order does violence also the natural and the moral order."

Ethics and Art

- Art – stands for beauty
- Ethics – stands for moral goodness
- "But as transcendental, the beauty and the good are ONE. Evil always implies ugliness or defect and the good is always beautiful since is it the very object of desire and therefore, like beauty, pleases when perceived."

Ethics and Politics

- Politics aim at good government for the temporal welfare of the citizens/
- Politics has often become very dirty and the reason is precisely because it is divorced from ethics.

Ethics and Education

- Education develops the whole man; his moral, intellectual and physical capacities. All should develop good moral character, personal discipline, civic consciousness, etc.

Morality and other Phases of Life

1. **Morality and Law –** morality and law are intimately related. Right and wrong, good and bad in human actions presuppose a law or rule of conduct.
   - The legal only covers the external acts of man;
   - The moral governs even the internal acts of man such as: volitional and the intentional activities of the will and mind.
     - Ex. Man's thoughts and desires
2. **Ethics and Religion –** the closest phase of life related to ethics.
   - Both of these are based on the following postulates:
     - The existence of the creator
     - Freedom of the will in man
     - Immorality
   - Both are the same end – the attainment of man's supreme purpose of man's ultimate end
   - Both prescribe the same means for attaining the goal of man: Right Living
   - "Some would divorce morality from religion, but religion is the root without which the plant of morality will die."

Importance of Ethics

- "Ethics is an indispensable knowledge. Without moral perception, man is only an animal. Without morality, man as rational being is a failure."
- Moral integrity is the only true measure of what man ought to be
- Morality is the foundation of every human society. Every culture admits the importance of morality as a standard of behaviours.

Importance of Integrity

- Integrity is a cornerstone of ethical behaviour.
- 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

I. MODIFIERS OF HUMAN ACT

Definition

- Things that may affect human acts in the essential qualities of knowledge, freedom, voluntariness and so make them less perfectly human.

- Factors that influence man's inner disposition towards certain actions
- They affect the mental or emotional state of a person to the extent that the voluntariness involved in an act is either increased or deceased

1. **Ignorance**
   - Absence of intellectual knowledge which a person ought to possess. In the realm of morals, everyone of age and reason is expected to know at least the general norms of good behaviour
   - **Vincible Ignorance ("conquerable")** – can easily be reminded through ordinary diligence and reasonable efforts. **Affected ignorance** – category of vincible ignorance in which a person keeps by positive efforts in order to escape responsibility or blame. Intentionally and willingfully maintaining ignorance.
   - **Invincible Ignorance ("unconquerable")** – type which a person possesses without being aware of it, or having awareness of it, lacks the means to rectify it. e.g. A person acts without realizing certain facts

2. **Passions/Concupiscence**
   - Either tendencies towards desirable object, or tendencies away from undesirable or harmful things.
   - The former are called positive emotions; the latter, negative emotions.
     - Positive emotions – love, desire, delight, hope, bravery, etc.
     - Negative emotions – hatred, horror, sadness, despair, fear, anger, etc.

3. **Fear**
   - Shrinking back of the mind from danger. It is the agitation of mind brought about by the apprehension of impending evil.
   - Distinction is made between an act done with fear and an act done out of or because of fear

Acts done with fear	Acts done out of fear
Embarking on a long journey	Child reads his book out of fear of the mother
Being left alone in a strange place	Employee volunteers to work overtime out of fear of being fired by the boss
Being asked to speak before a group of people	Friend stops smoking out of fear of contracting cancer

4. **Habit**
   - Lasting readiness and facility born of frequently repeated acts, for acting in a certain manner
   - Habits are acquired inclinations towards something to be done
   - They assume the role of a second nature, moving one who has them to perform certain acts with relative ease

5. **Violence**
   - External force applied by a free cause for the purpose of compelling a person to perform an act which is against his will
   - Any physical force exerted on a person by another free agent for the purpose of compelling said person to act against his will
   - Bodily torture, maltreatment, isolation, and mutilation – are examples of violence against persons.

Ethics vs. Law

- Law – a systematic body of riles that governs the whole society and the actions of its individual members.
- Ethics – a branch of moral philosophy that guides people about the basic human conduct

More the RIGHT and WRONG

- Students frequently equate ethical with legal. Often see a situation in Black and White.
- Ethical Decision Making and Information Technology (1993)
  - Legal/Ethical
  - Not Legal/Ethical
  - Legal/Not Ethical
  - Not Legal/Not Ethical

II. ETHICS FOR IT PROFESSIONALS AND IT USERS

What exactly is a PROFESSION?

- A profession can be understood in terms of the attributes and requirements of a professional practice, such as "calling in which special knowledge and skill are used in…the service of mankind." (Firmage, 1991)
- Greenwood (1991) believes that professions are occupational fields distinguishable in terms of five characteristics: (i) systematic theory, (ii) authority, (iii) community sanction. (iv) ethical codes, and (v) a culture

What is Professional Ethics?

- When applied to computing, professional ethics is a field of applied ethics concerned with moral issues that impact computer professionals.

Why separate category for professional ethics?

- The same ethical rule involving honesty, fairness, and so forth should apply to professional as well as to ordinary individuals
- So, if it is wrong for ordinary people to steal, cheat, lie and so forth, then it is wrong for professionals to do so as well.

Who is PROFESSIONAL?

- A professional is a member of a profession or any person who earns their living from a specified professional activity
- Those who comprise a given profession also tend to have certain defining attributes and requirements
- Computer Professional – anyone who is employed in the computer, IT or any IT related fields.

IT Professionals

- Profession is a calling that requires:
  - Specialized knowledge
  - Long and intensive academic preparation

Are IT Workers Professionals?

- Partial list of IT Specialist:
  1. Programmers
  2. Systems Analysts
  3. Software Engineers
  4. Database Admins
  5. Network Admins

6. CIOs

- Legal Perspective
  1. IT workers are not recognized as professionals
  2. Not licensed
  3. IT workers are not liable for malpractice

Professional Relationships that must be managed:

- IT Professionals have many different relationships with:
  1. Employers
  2. Clients
  3. Suppliers
  4. Other IT Professionals
  5. IT users
  6. Society at large

Professional Code of Ethics

- A professional code of ethics states that principles and core values that are essential to the work of a particular occupational group.
- Main parts:
  - Outlines what the professional organization aspires to become
  - Lists if rules and principles by which members of the organization are expected to abide
- Benefits for individual, profession, and society
  - Improves ethical decision making
  - Promotes high standards of practice and ethical behaviour
  - Enhances trust and respect from the general public
  - Provides an evaluation of benchmark

Professional Organizations

- No universal code of ethics for IT professionals
- No single, formal organization of IT professionals has emerged as preeminent
- Most prominent organization include:
  - Association of Computing Machinery (ACM)
  - Association of Information Technology Professionals (AITP)
  - Computer Society of the Institute of Electrical and Electronics Engineers (IEEE-CS)
  - Project Management Institute (PMI)

Purpose of Professional Codes

- Professional codes of ethics are often designed to motivate members of an association to behave in certain ways.
- Four primary functions of codes are to:
  - Inspire
  - Guide
  - Educate
  - Discipline the members

The ACM/IEEE Code of Ethics

Software Engineering Code of Ethics and Professional Practice

ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices

8 Principles in Code of Ethics

1. **Public** – Software engineers shall act consistently with the public interest
2. **Client and Employer** – Software engineers shall act in a manner that is in the best of interest of their client and employer consistent with the public interest
3. **Product** – Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. **Judgement** – Software engineers shall maintain integrity and independence in their professional judgement.
5. **Management** – Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance
6. **Profession** – Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. **Colleagues** – Software engineers shall be fair to and supportive of their colleagues
8. **Self** – Software engineers shall participate in a lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession

Certification

- Indicates a professional possesses a particular set of skills, knowledge, or abilities in the opinion of a certifying organization
- Can also apply to products
- Generally voluntary
- Carries no requirement to adhere to a code of ethics

1. **Vendor Certifications:**
   - Some certifications substantially improve IT workers' salaries and career prospects
   - Relevant for narrowly defined roles; or certain aspects of broader roles
   - Require passing a written exam
   - Workers are commonly recertified as newer technologies become available
2. **Industry Association Certifications:**
   - Require a certain level of experience and a broader perspective than vendor certifications
   - Lag in developing tests that cover new technologies

Government Licensing

- Case for licensing IT professionals:
  1. Encourage IT professionals to follow the highest standards of the profession
  2. Practice a code of ethics
  3. Violators would be punished
- Issues associated with gov't licensing of IT professionals:
  - There are few international or national licensing programs for IT professionals
  - No universally accepted core body of knowledge
  - Unclear who should manage content and administration of licensing exams
  - No administrative body to accredit professional education programs
  - No administrative body to assess and ensure compensation of individual professionals

IT Professional Malpractice

- Negligence has been defined as not doing something that a reasonable man would do, or doing something that a reasonable man would not do
- Duty of care refers to the obligation to protect people against any unreasonable harm or risk
- Courts consistently reject attempts to sue individual parties for computer-related malpractice

Ethical Guidelines for Computer Professionals

1. Understand what success means
2. Include user (such as medical staff, technicians, pilots, office workers) in the design and testing stages to provide safe and useful systems
3. Do a thorough, careful job when planning and scheduling a project and when writing bids or contracts
4. Design for real users

Common Ethical Issues for IT Users

1. **Privacy**
   - Most people have their personal data spread throughout the digital world. Even things thought to be secure, such as email or private accounts, can be accessed by unintended sources
   - Most employers actively check their employees' computer habits. Privacy has evolving legal implications, but there are also ethical considerations
2. **Digital Ownership**
   - Digital mediums have allowed information to flow more freely than before. This exchange of ideas come with a legal and ethical backlash
   - How can ownership be established in the digital realm? Things can be easily copied and pasted online, which makes intellectual property hard to control
3. **Data Gathering**
   - The United States has even passed legislation allowing the government to actively monitor private citizens in the name of national security
   - These measures have revived a debate about what information can be gathered and why. This debate applies on a smaller scale as well because companies need to consider what information to collect from their employees.
4. **Security Liability**
   - Security systems for digital networks are computerized in order to protect vital information and important assets. However, this increased security comes with increased surveillance
   - All security systems have inherent risks, which means it is a question of what risks are acceptable and what freedoms can be forfeited.
   - Ultimately, IT professionals need to balance risk with freedom to create a security system that is effective an ethical at the same time
5. **Access Costs**
   - Net neutrality has become a trendy issue thanks to legislative efforts in the last few years. The issue of net neutrality is essentially a question of access.
   - Proponents want the Internet to remain open to everyone while some businesses want to create tiered access for those who are willing to pay. The issue even extends to private Internet usage since the cost of service in some areas may be cost prohibitive.

What is Cyber-ethics?

- Cyberethics is the study of moral, legal, and social issues involving cybertechnology.
- It examines the impact that cybertechnology has for our social, legal, and moral systems.
- It also evaluates the social policies and laws that have been framed in response to issues generated by the development and use of cybertechnology.

What is Cybertechnology?

- Cybertechnology refers to a wide range of computing and communications devices - from standalone computers, to "connected" or networked computing and communications technologies, to the Internet itself.
- Cybertechnologies include: hand-held device (such as Palm Pilots), personal computers (desktops and laptops), mainframe computers, and so forth.

Ten Commandments of Cyber

- Thou shalt not use a computer to harm other people.
- Thou shalt not interfere with other people's computer work.
- Thou shalt not snoop around in other people's files.
- Thou shalt not use a computer to steal.
- Thou shalt not use a computer to bear false witness.
- Thou shalt not use or copy software for which you have not paid.
- Thou shalt not use other people's computer resources without authorization.
- Thou shalt not appropriate other people's intellectual output.
- Thou shalt think about the social consequences of the program you write.
- Thou shalt use a computer in ways that show consideration and respect.

Supplemental Reading

<u>Professional Codes of Ethics</u>

A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group. Practitioners in many professions subscribe to a code of ethics that governs their behavior. For example, doctors adhere to varying versions of the 2,000-year-old Hippocratic oath, which medical schools offer as an affirmation to their graduating classes. Most codes of ethics created by professional organizations have two main parts: The first outlines what the organization aspires to become, and the second typically lists rules and principles by which members of the organization are expected to abide. Many codes also include a commitment to continuing education for those who practice the profession.

Laws do not provide a complete guide to ethical behavior. Just because an activity is not defined as illegal does not mean it is ethical. Nor can a professional code of ethics be expected to provide an answer to every ethical dilemma—no code can be a definitive collection of behavioral standards. However, following a professional code of ethics can produce many benefits for the individual, the profession, and society as a whole:

Ethical decision making—Adherence to a professional code of ethics means that practitioners use a common set of core values and beliefs as a guideline for ethical decision making.

High standards of practice and ethical behavior—Adherence to a code of ethics reminds professionals of the responsibilities and duties that they may be tempted to compromise to meet the pressures of day-to-day business. The code also defines acceptable and unacceptable behaviors to guide professionals in their interactions with others. Strong codes of ethics have procedures for censuring professionals for serious violations, with penalties that can include the loss of the right to practice. Such codes are the exception, however, and few exist in the IT arena.

Trust and respect from the general public—Public trust is built on the expectation that a professional will behave ethically. People must often depend on the integrity and good judgment of a professional to tell the truth, abstain from giving self-serving advice, and offer warnings about the potential negative side effects of their actions. Thus, adherence to a code of ethics enhances trust and respect for professionals and their profession.

Evaluation benchmark—A code of ethics provides an evaluation benchmark that a professional can use as a means of self-assessment. Peers of the professional can also use the code for recognition or censure.

The Case for Licensing IT Workers

The days of simple, stand-alone information systems are over. Modern systems are highly complex, interconnected, and critically dependent on one another. Highly integrated enterprise resource planning (ERP) systems help multibillion-dollar companies control all of their business functions, including forecasting, production planning, purchasing, inventory control, manufacturing, and distribution. Complex computers and information systems manage and control the nuclear reactors of power plants that generate electricity. Medical information systems monitor the vital statistics of hospital patients on critical life support. Every year, local, state, and federal government information systems are entrusted with generating and distributing millions of checks worth billions of dollars to the public.

As a result of the increasing importance of IT in our everyday lives, the development of reliable, effective information systems has become an area of mounting public concern. This concern has led to a debate about whether the licensing of IT workers would improve information systems. Proponents argue that licensing would strongly encourage IT workers to follow the highest standards of the profession and practice a code of ethics. Licensing would also allow for violators to be punished. Without licensing, there are no clear, well-defined requirements for heightened care and no concept of professional malpractice.

Issues Associated with Government Licensing of IT Workers

Australia, Great Britain, and the Canadian provinces of Ontario and British Columbia have adopted licensing for software engineers. In the United States, the National Council of Examiners for Engineering and Surveying (NCEES) has developed a professional exam for electrical engineers and computer engineers. However, there are many reasons why there are few international or national licensing programs for IT workers in the United States:

There is no universally accepted core body of knowledge. The core body of knowledge for any profession outlines agreed-upon sets of skills and abilities that all licensed professionals must possess. At present, however, there are no universally accepted standards for licensing programmers, software engineers, and other IT workers. Instead, various professional societies, state agencies, and federal governments have developed their own standards.

It is unclear who should manage the content and administration of licensing exams. How would licensing exams be constructed, and who would be responsible for designing and administering them? Would someone who passes a license exam in one state or country be accepted in another state or country? In a field as rapidly changing as IT, workers must commit to ongoing, continuous education. If an IT worker's license were to expire every few years (like a driver's license), how often would practitioners be required to prove competence in new practices in order to renew their license? Such questions would normally be answered by the state agency that licenses other professionals.

There is no administrative body to accredit professional education programs. Unlike the American Medical Association for medical schools or the American Bar Association for law schools, no single body accredits professional education programs for IT. Furthermore, there is no well-defined, step-by-step process to train IT workers, even for specific jobs such as programming. There is not even broad agreement on what skills a good programmer must possess; it is highly situational, depending on the computing environment.

There is no administrative body to assess and ensure competence of individual workers. Lawyers, doctors, and other licensed professionals are held accountable to high ethical standards and can lose their license for failing to meet those standards or for demonstrating incompetence. The AITP standards of conduct state that professionals should "take appropriate action in regard to any illegal or unethical practices that come to [their] attention. However, [they should] bring charges against any person only when [they] have reasonable basis for believing in the truth of the allegations and without any regard to personal interest." The AITP code addresses the censure issue much more forcefully than other IT codes of ethics, although it has seldom, if ever, been used to censure practicing IT workers.

IT Professional Malpractice

Negligence has been defined as not doing something that a reasonable person would do, or doing something that a reasonable person would not do. Duty of care refers to the obligation to protect people against any unreasonable harm or risk. For example, people have a duty to keep their pets from attacking others and to operate their cars safely. Similarly, businesses must keep dangerous pollutants out of the air and water, make safe products, and maintain safe operating conditions for employees. The courts decide whether parties owe a duty of care by applying a reasonable person standard to evaluate how an objective, careful, and conscientious person would have acted in the same circumstances. Likewise, defendants who have particular expertise or competence are measured against a reasonable professional standard. For example, in a medical malpractice suit based on improper treatment of a broken bone, the standard of measure would be higher if the defendant were an orthopedic surgeon rather than a general practitioner. In the IT arena, consider a hypothetical negligence case in which an employee inadvertently destroyed millions of customer records in an Oracle database. The standard of measure would be higher if the defendant were a licensed, Oracle certified database administrator (DBA) with 10 years of experience rather than an unlicensed systems analyst with no DBA experience or specific knowledge of the Oracle software.

If a court finds that a defendant actually owed a duty of care, it must then determine whether the duty was breached. A breach of the duty of care is the failure to act as a reasonable person would act. A breach of duty might consist of an action, such as throwing a lit cigarette into a fireworks factory and causing an explosion, or a failure to act when there is a duty to do so—for example, a police officer not protecting a citizen from an attacker.

Professionals who breach the duty of care are liable for injuries that their negligence causes. This liability is commonly referred to as professional malpractice. For example, a CPA who fails to use reasonable care, knowledge, skill, and judgment when auditing a client's books is liable for accounting malpractice. Professionals who breach this duty are liable to their patients or clients, and possibly to some third parties.

Courts have consistently rejected attempts to sue individual parties for computer related malpractice. Professional negligence can only occur when people fail to perform within the standards of their profession, and software engineering is not a uniformly licensed profession in the United States. Because there are no uniform standards against which to compare a software engineer's professional behavior, he or she cannot be subject to malpractice lawsuits.

III. SECURITY AND PRIVACY

Introduction

- The ubiquitous use of computers and technology prompts some very important questions about the use of personal data and our right to privacy & security.
- Privacy and security are related. Privacy relates to any rights you have to control your personal information and how it's used. Security, on the other hand, refers to how your personal information is protected

PRIVACY

What is Privacy?

- The state or condition of being free from being observed or disturbed by other people.
- The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively
- The right of an individual to be secure from unauthorized disclosure of information about oneself.
- Privacy is the ability of a person to control the availability of information about and exposure of himself or herself.
- The right to be "left alone"

Types of PRIVACY

1. **Physical –** preventing "intrusions into one's physical space or solitude."
   - Some issues concerning physical privacy
     - Trespassing
     - Stalking
     - Surveillance
2. **Informational –** is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one's personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use)
   - Topics associated with informational privacy
     - Internet privacy
     - Cable television
     - Medical
     - Financial
     - Political
3. **Organizational –** Governments agencies, corporations, and other organizations may desire to keep their activities or secrets from being revealed to other organizations or individuals.
   - Coverage of organizational privacy
     - Patents
     - Classified Information
     - Trade Secrets

Privacy as a Human Right
Philippine Constitution: Bill of Rights
Article 3 Section 2

- The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

Article 3 Section 3

1. The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.
2. Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.

Article 26 of the Civil Code

- Every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons. The following and similar acts, though they may not constitute a criminal offense, shall produce a cause of action for damages, prevention and other relief:

1. Prying into the privacy of another's residence.
2. Meddling with or disturbing the private life or family relations of another.
3. Intriguing to cause another to be alienated from his friends.
4. Vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical defect, or other personal condition.

Article 32 of the Civil Code

- "Any public officer or employee, or any private individual, who directly or indirectly obstructs, defeats, violates or in any manner impedes or impairs the privacy of communication and correspondence shall be liable for damages."

United Nations' Declaration of Human Rights
Article 12: The Right to Privacy

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Philippine Data Protection Framework

The Government Data Privacy Protection Act seeks to protect personally identifiable information held by government agencies. The bill requires agencies to use reliable encryption for databases. Agencies must also secure the necessary contractual obligations from private contractors who might access or participate in the data processing. Access to sensitive data, such as financial information, requires security clearance, and off-site access requires approval by the head of the government agency.

Section 2.3
Guidelines for the Protection of Personal Data in Information and Communications System in the Private Sector

1. Collection and processing of personal data are for specified and legitimate purposes
2. Data is processed fairly, accurately and lawfully
3. Information is up to date and accurate in every respect
4. Data is retained only for as long as necessary to fulfill the purpose for which it is collected
5. The data subjects have rights to access, rectify and ensure the destruction of the data.

Invasion of Privacy

The intrusion into the personal life of another, without just cause, which can give the person whose privacy has been invaded a right to bring a lawsuit for damages against the person or entity that intruded.

1. **Intrusion of Solitude** – actual physical or electronic penetration of a person's private home or other personal space.
2. **Public disclosure of private facts** – the facts themselves may be completely true, but the method of obtaining those facts and publishing them could constitute an invasion of privacy.
3. **Publicity which puts a person in false light** – whenever someone deliberately misrepresents the "character, history, activities or beliefs" of another person.
4. **Appropriation of one's name or picture for personal or commercial advantage** – unauthorized use of a person's picture to advertise certain products.

Technology as a Threat to Privacy

1. **Malware** – malicious program planted into your computer without your consent
2. **Internet scams** – Phishing, Spear Phishing, Whaling, etc.
3. **Social Media Risks** – sharing info, cyberbullying, libel, etc.
4. **Web Browser History** – your online footprints are always recorded in your browser. Hackers can get into this information to reveal detailed information about yourself.
5. **Ads & Cookies** – advertisements eagerly collect all soft of personal data about us; companies gather information by dropping small files.
6. **The Cloud** – high change of attracting malicious hackers.
7. **Public Wi-Fi** – potential stage for hackers.

Tips of Increasing Online Privacy

- Understand privacy policies on web sites.
- Use a separate account for your personal e-mail.
- Control who sees your information.
- Clear your browser cache after browsing.
- Make sure that online forms are secure.
- Reject unnecessary cookies.
- Use encryption.
- Use "anonymity" while browsing.
- Opt-out of third-party information sharing.
- Research, join forums, and stay informed

SECURITY

What is SECURITY?

- Refers to how your personal information is protected.
- The state of being free from danger or threat.
- Safety; measure taken to be safe or protected
- Protecting important data, confidential information, networks, software, equipment, facilities, company's assets, and personnel is what physical security is about.

Some questions about SECURITY

- Where is my data?
- How is it used?
- Who sees it?
- Is anything private anymore?

How did they get my data?

- Loans
- Charge accounts
- Orders via mail
- Magazine subscriptions
- Tax forms
- Applications for schools, jobs, clubs
- Insurance claim
- Hospital stays
- Sending checks
- Fund-raisers
- Advertisers
- Warranties
- Military draft registration
- Court petition

Your BOSS is monitoring you!

Monitoring Software for:

- Screens
- E-mail
- Keystrokes per minute
- Length of breaks
- What computer files are used and for how long

Monitoring by Web Sites

Records:

- City or site you just left
- Everything you do while on the site
- Hardware and software you use

Cookie:

- Stores information about you located on your hard drive
- Beneficial uses: viewing preferences, online shopping, secure sites retain password in cookie
- Controversial: tracking surfing habits for advertisers

Security and Privacy

Data communication capabilities provides new challenges:

Keep data secure

- Destruction
- Accidental damage
- Theft
- Espionage

Keep data private

- Salaries
- Medical information
- Social security numbers

- Bank balances

- making regular **backups** of files (backup copies should be stored in fireproof safes or in another building)
- protecting yourself against **viruses** by running **anti-virus software**
- using a system of passwords so that access to data is restricted
- safe storage of important files stored on **removable disks**, e.g. locked away in a fireproof and waterproof safe
- allowing only authorized staff into certain computer areas, e.g. by controlling entry to these areas by means of ID cards or magnetic swipe cards
- always logging off or turning **terminals** off and if possible locking them
- avoiding accidental deletion of files by **write-protecting** disks
- using data **encryption** techniques to code data so that it makes no apparent sense

Security: Safeguards Systems

System of safeguard designed to protect a computer system and data from deliberate or accidental damage

- Natural Disasters
- Fire
- Accidents
- Vandalism
- Theft or destruction of data
- Industrial espionage
- Hackers

Identification and Access

- Provide access to authorized individuals only
- Uses one or more of the following systems:
    - What you have
    - What you know
    - What you do
    - What you are
- **Internal controls** – transaction logs
- **Auditor checks** – who has accessed data during periods when that data is not usually used?
- **Secured waste** – shredders, locked trash barrels
- **Applicant screening** – verify the facts on a resume, background checks
- **Built-in software protection** – record unauthorized access attempts; user profile

Security: The Internet

- **Firewall** – device that governs interaction between internal network and the internet; NGFW, IPS/IDS, AMP, VPN
- **Encryption** – DES, 3DES, AES, IDEA
- Whitelisting/Blacklisting of websites
- Use of TOR

Security: Personal Computers

- Physical security with locks and cables
- Surge protector
- UPS
- Back-up files regularly and systematically

Disaster Recovery

- An area of security planning that aims to protect an organization from the effects of significant negative events. DR allows an organization to maintain or quickly resume mission-critical functions following a **disaster**.
- **Hardware Loss:** Can be replaced and temporarily diminished processing ability.
- **Software Loss:** Industry standard to make backups of program files
- **Data Loss:** reassemble records

Disaster Recovery includes:

- Priorities for programs
- Plans for notifying employees
- List of needed equipment and where it is located
- Alternative computing facilities
- Procedures for handling input and output data
- Emergency drills

Supplemental Reading

When it comes to privacy and security, it's a good idea to have both. Each can impact your cyber safety. But what's the difference?

Privacy and security are related. Privacy relates to any rights you have to control your personal information and how it's used. Think about those privacy policies you're asked to read and agree to when you download new smartphone apps.

Security, on the other hand, refers to how your personal information is protected. Your data — different details about you — may live in a lot of places. That can challenge both your privacy and your security.

Some people regard privacy and security as pretty much the same thing. That's because the two sometimes overlap in a connected world. But they aren't the same, and knowing how they differ may help you to protect yourself in an increasingly connected world.

What's the difference between privacy and security?

Here's an example. You might share personal information with your bank when you open a checking account. What happens after that? Here are three possible outcomes, all related to your personal information (not to the money you may have deposited in the checking account).

Your privacy and security are maintained. The bank uses your information to open your account and provide you with products and services. They go on to protect that data.

Your privacy is compromised, and your security is maintained. The bank sells some of your information to a marketer. Note: You may have agreed to this in the bank's privacy disclosure. The result? Your personal information is in more hands than you may have wanted.

Both your privacy and security are compromised. The bank gets hit by a data breach. Cybercriminals penetrate a bank database, a security breach. Your information is exposed and could be sold on the dark web. Your privacy is gone. You could become the victim of cyber fraud and identity theft.

It would be great if your risks began and ended with that theoretical bank. But your personal information is likely all over the connected world — in government offices, at healthcare providers, at stores and restaurants, and in many of your online accounts. You might say it's everywhere — not literally, but it's certainly in enough places that it's out of your control.

If a cybercriminal accesses that information, it could be off to the races. Your privacy and security could both get trampled.

What's the difference between privacy and security in the online world?

Cybersecurity products can help protect your privacy and security — sometimes at the same time.

For instance, consider a VPN — a virtual private network. It's a security product that acts like a tunnel for your information and your activity on the internet, encrypting all the data that you send or receive on your device. It’s like an online version of sitting with your back to a wall when you don’t want someone else to see what you’re doing on your computer or phone when you’re at a café or airport.

Here’s how a VPN helps you win two ways:

Privacy: It helps to block websites, internet browsers, cable companies, and internet service providers from tracking your information and your browser history.

Security: It helps protect you from other people accessing your personal information and other data