POLYTECHNIC UNIVERSITY OF THE PHILIPPINES
COLLEGE OF COMPUTER AND INFORMATION SCIENCES
DEPARTMENT OF COMPUTER SCIENCE | DEPARTMENT OF INFORMATION TECHNOLOGY

IT SOCIAL ISSUES AND PROFESSIONAL ISSUES

INSTRUCTIONAL MATERIAL FOR STUDENTS

Prepared by:

Domingo, IVR, Yu-Miclat, S., Hogar-Reyes, ME.

Course Title : **IT SOCIAL AND PROFESSIONAL ISSUES**

Course Code : **INTE 4203**

Course Credit : **3 UNITS / 3 HOURS**
Pre-Requisite :

Course Description : This course introduces the students to the social and professional issues surrounding the development and use of Information Communication Technologies (ICTs) in the 21st century. This course examines the pervading presence of IT in various professions and its impact on the lives and social culture of people, whether in Medicine, Business, Entertainment and Education. The course covers topics on the enabled industries, Internet Censorship and Freedom of Expression, Sex and Technology, Technology and Privacy, Information Warfare, E-Health, Online Crimes, E-Lifestyle, and E-Learning and Distance Education.

INSTITUTIONAL INTENDED LEARNING OUTCOMES (ILO)	**PROGRAM INTENDED LEARNING OUTCOMES (PILO) COLLEGE**		**COURSE INTENDED LEARNING OUTCOMES (CILO) SUBJECT**
	BSIT	BSIT Graduate Outcomes	Course Outcomes
Creative and Critical Thinking	IT01	Apply knowledge of computing, science, and mathematics appropriate to the discipline.	Learn the current issues surrounding the development and use of ICTs Evaluate the positive and negative side of a critical IT-related issues Learn the risks involved in using ICT, as well as, the protection and security measures to avoid becoming victims of cybercrimes Identify emerging and converging technologies, including trends in hardware, software and data security Develop cooperation in group discussion, research activities and presentations Present the Pros and Cons of ICT's societal impact Discuss the important role of ICTs in the improvement of the modern society, as well as its effects in the evolving the culture of things Imbue the value of integrity and moral responsibility as a future ICT Professional Uphold and improve IT professional standards thru continuing education and personal development
	IT03	Analyze complex problems, and identify and define the computing requirements appropriate to its solution.	
	IT05	Design, implement, and evaluate computer based systems, processes, components, or programs to meet desired needs and requirements under various constraints.	
	IT06	Integrate IT-based solutions into the user environment effectively.	
	IT09	Assist in the creation of an effective IT project plan.	
Adeptness in the Responsible Use of Technology Community Engagement	IT07	Apply knowledge through the use of current techniques, skills, tools and practices necessary for the IT profession	
	IT02	Understand best practices and standards and their applications.	
High Level of Leadership and Organizational Skills. Strong Service Orientation	IT08	Function effectively as a member or leader of a development team recognizing the different roles within a team to accomplish a common goal.	
Effective Communication	IT10	Communicate effectively with the computing community and with society at large about complex computing activities through logical	

		writing, presentations, and clear instructions.	
Sense of Nationalism and Global Responsiveness.	IT11	Analyze the local and global impact of computing information technology on individuals, organizations, and society.	
Sense of Personal and Professional Ethics	IT12	Understand professional, ethical, legal, security and social issues and responsibilities in the utilization of information technology.	
Passion to Life-Long Learning	IT13	Recognize the need for and engage in planning self-learning and improving performance as a foundation for continuing professional development.	

Week	Topic	Learning Outcomes	Methodology	Assessment
Week 1	Course Orientation	Knowledge of expectations and requirements of the course.	Lecture	
Week 2	1. Global Digital Environment 1.1 Globalization 1.2 The Digital Divide 1.3 Information System Trends	Analyze the local and global impact of computing information technology on individuals, organizations and society	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination / Research
Week 3	2. Emerging and Converging Information Communication Technologies 2.1 Emerging Software Technologies 2.2 Miniaturized and Multifunctional Machines 2.3 The Rise of Robotics	Identify and utilize emerging and converging technologies	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination
Week 4	3. ICT-enabled Industry 3.1 Business Process Outsourcing 3.2 Mobile-based Service Industry 3.3 E-Services/E-Government	Design, implement and evaluate computer-based systems, processes, components, or programs to meet desired needs and requirements Identify options for future job opportunities Identify the different ways to have a sustainable professional career	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination and Research
Week 5	4. Internet Censorship and Freedom of Expression 4.1 Website Content Filtration 4.2 Censorship vs Regulation	Analyze and decide on boundaries between what is legal or not	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination and Research
Week 6	5. Sex and Technology 5.1 Child Pornography 5.2 Virtual Prostitution 5.3 Cyber Sex 5.4 Online Relationships	Analyze complex problems, and identify and define the computing requirements appropriate to its solution	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination /Analysis Case Work and Research
Week 7	6.Technology and Privacy 6.1 Identity Theft/Impersonation 6.2 Monitoring vs Intrusion to Privacy	Understand professional, ethical, legal, security and social issues and responsibilities in the utilization of information technology	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination and Research

Week 8	7. Information Warfare 7.1 Cyber Espionage 7.2 Intelligence Gathering	Understand professional, ethical, legal, security and social issues and responsibilities in the utilization of information technology	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination and Research
Week 9	Midterm Examination			
Week 10	8. E-Health 8.1 Telemedicine 8.2 Virtual Therapy	Identify and analyze user needs and take them into account in the selection, creation, evaluation and administration of computer-based systems	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination and Research
Week 11-12	9. Online Crimes 9.1 Hacking 9.2 Spamming 9.3 Technology-based Terrorism 9.4 Online Fraud	Understand professional, ethical, legal, security and social issues and responsibilities in the utilization of information technology	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination and Research
Week 13-14	10. E-Lifestyle 10.1 SMS Addiction 10.2 Online and Network-based Gaming 10.3 Online Shopping 10.4 Blogging, Social Networks and Personal Websites 10.5 Home-based and Mobile Offices	Integrate IT-based solutions into the user environment effectively Apply knowledge through the use of current technologies, skills, tools and practices	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination and Research
Week 15	11. E-Learning and Distance Education 11.1 Computer-based Training 11.2 Online Education/Distance Learning	Recognize the need for and engage in planning self-learning and improving performance as a foundation for continuing professional development	Lecture forum Demonstration Gapped lecture Study group Think aloud modeling	Recitation Seatwork / Homework Examination and Research
Week 16	Case Analysis			
Week 17	Final Examination			
Week 18	Round-up Activities			

Grading System:

Midterm Grade =70% Class Standing (Quizzes, Recitation, Assignment, Attendance, Research Work); 30% Midterm Examination

Second Grading = 70% Class Standing (Quizzes, Recitation, Assignment, Attendance, Research Work, Case Study); 30% Final Examination

Final Grade = (Midterm Grade + Second Grading) / 2
Passing mark is 60% of the total number of items

General Rules:

Aside from what is prescribed in the student handbook, the following are the professor's additional house rules: :

1. Assignments and research projects/report works will be given throughout the semester. Such requirements shall be due as announced in class. Late submission shall be penalized with grade deductions (5% per day) or shall no longer be accepted, depending on the subject facilitator's discretion. Assignments and exercises are designed to assist you in understanding the materials presented in class, and to prepare you for the exams.
2. Students are required to attend classes regularly, including possible make-up classes. The student will be held liable for all topics covered and assignments made during his/her absence. The university guidelines on attendance and tardiness will be implemented. Every meeting, an attendance sheet will be passed around. Be sure to sign it.
3. Academic honesty should be practiced at all times. Any evidence of copying or cheating on any course work may result in a failing grade for all parties involved.
4. Students are advised to keep graded work until the semester has ended.

	5. Contents of the syllabus are subject to modification with notification. 6. Cell phone, radio or other listening devices are not allowed to be used inside lecture and laboratory rooms to prevent any distractive interruption of the class activity. 7. No food, drinks, cigarettes, nor children are allowed inside the lecture and laboratory rooms. 8. Only officially enrolled students are allowed inside the lecture or laboratory room. Withdrawal and dropping of the subject should be done in accordance with existing university policies and guidelines.

References:

1. Lavina, Erise, et.al. Ethics for I.T. Professionals with Legal Aspects in Computing, 2012.
2. Tavani. Ethics and Technology, 2011.
3. Whitmat, Michael & Mattord. Reading and Cases in the Management of Information Security, 2006.
4. Baase, Sara. A Gift of Fire: Social, Legal and Ethical Issues for Computing and the Internet, 2008
5. Talabis, Mark, et.al. Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data, 2015.
6. Harris, Charles E., et.al. Engineering Ethics: Concepts and Cases, 2014.
7. Minelli, Michael, Chambers, Michelle & Dhiraj, Ambiga. Big Data, Big Emerging Business Intelligence and Analytic Trends for Today's Businesses, 2013.
8. Whitney, Hunter. Data Insights: New Ways to Visualize and Make Sense of Data, 2013.
9. Procise. Incident Response: Investigating Computer Crime, 2001.
10. Hick, Ed. Human Rights and the Internet, 2000.

Prepared by:	Date:	Reviewed by:	Date:	Approved by:	Date
Maria Esperanza Hogar Reyes Course Specialist		Marian Arada Chairperson, Department of Information Technology		Benilda Comendador Dean, CCIS	

TABLE OF CONTENTS

CHAPTER 1. GLOBAL DIGITAL ENVIRONMENT

Overview: The Internet has wired the world. Today it is just as simple to communicate with someone on the other side of the world as it is to talk to someone next door. In this chapter, we will look at the implications of globalization and the impact it is having on the world.

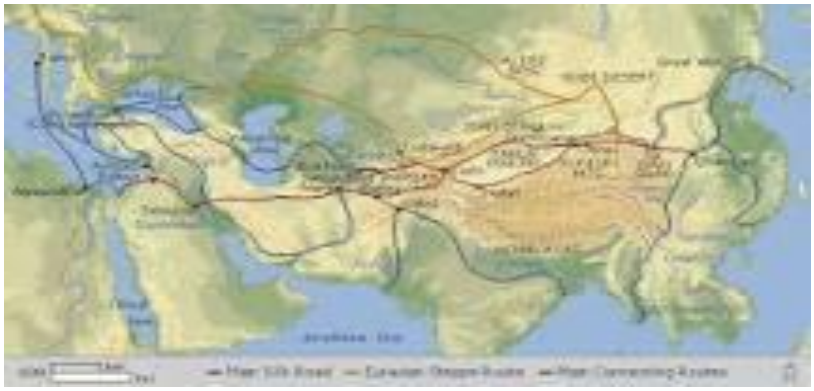
Learning Objectives:

At the end of the Chapter, the student must be able to:

- Analyze the local and global impact of computing information technology on individuals, organizations and society

1.1 GLOBALIZATION

Globalization is a process of interaction and integration among the people, companies, and governments of different nations, a process driven by international trade and investment and aided by information technology



1.2 DIGITAL DIVIDE

The ability to use and manipulate digitalized technology is very important which is why it is ideal for everyone to have a share of technology. The digital divide describes the problem we are faced with.

Digital Divide is the unequal access of information and communication technology between different groups of society, and the knowledge of the skills required to use the technology. Simply put, some people can use computers, some cannot. Either because they do not have one, or they have never been taught how.

People most affected include low socio-economic areas, developing countries, rural women and children. In Africa, only 3% of the population has internet. In Asia, 1% of the

population in Cambodia, Laos and Bangladesh has internet. The Middle East accounts for 0.9% of global Internet users.

The question is: What are we doing to close the gap?

1.3 INFORMATION SYSTEMS TRENDS

a. Cloud Computing

Cloud computing is a network of resources a company can access, and this method of using a digital drive increases the efficiency of organizations. Instead of local storage on computer hard drives, companies will be freeing their space and conserving funds. According to Forbes, 83 percent of enterprise workloads will be in the cloud by 2020, which means 2019 will show an increasing trend closing in on this statistic.

Cloud storage and sharing is a popular trend many companies have adopted and even implemented for employee interaction. A company-wide network will help businesses save on information technology infrastructure. Cloud services will also extend internal functions to gain revenue. Organizations that offer cloud services will market these for external products and continue their momentum.

Organizations will transfer their stored files across multiple sources using virtualization. Companies are already using this level of virtualization, but will further embrace it in the year to come. Less installation across company computers is another positive result of cloud computing because the Internet allows direct access to shared technology and information. The freedom of new products and services makes cloud computing a growing trend.

b. Mobile Computing and Applications

Mobile phones, tablets, and other devices have taken both the business world and the personal realm by storm. Mobile usage and the number of applications generated have both skyrocketed in recent years.

c. Big Data Analytics

Big data is a trend that allows businesses to analyze extensive sets of information to achieve variety in increasing volumes and growth of velocity. Big data has a high return on investment that boosts the productivity of marketing campaigns, due to its ability to enable high-functioning processing. Data mining is a way companies can predict growth opportunities and achieve future success. Examination of data to understand markets and strategies is becoming more manageable with advances in data analytic programs.

d. Automation

Another current trend in the IT industry is automated processes. Automated processes can collect information from vendors, customers, and other documentation.

LET'S ASSESS WHAT YOU HAVE LEARNED:

Due to the global pandemic, different platforms are now being used in educational systems, thanks to the global digital environment. Teachers and students, on the other hand, are

both experiencing very poor internet connections as a result of the digital divide. What do you think the consequences and effects of the digital divide will be in our educational system?

CHAPTER 2. EMERGING AND CONVERGING INFORMATION COMMUNICATION TECHNOLOGIES

Overview: While nanotechnology (and all other **emerging**, **converging technologies**) promise radical changes in science and society, future progress in the field will require overcoming many scientific challenges.

Learning Objectives:
At the end of the Chapter, the student must be able to:

- Identify and utilize emerging and converging technologies

2.1 EMERGING SOFTWARE TECHNOLOGIES

1. Artificial Intelligence and Smart Machines

Artificial intelligence harnesses algorithms and machine learning to predict useful patterns humans normally identify. Smart machines take human decision-making out of the equation so intelligent machines can instigate changes and bring forward solutions to basic problems. Companies are rallying around artificial intelligence in the workplace because it allows employees to use their abilities for the most worthwhile tasks, along with management of these smart machines for a more successful system.

2. Virtual Reality

Technology that includes virtual reality is becoming prevalent. The software of virtual reality is making many industries prepared for various scenarios before entering them. The medical profession is projected to use virtual reality for some treatments and interactions with patients in the coming years. Virtual training sessions for companies can cut costs, fill in the need for personnel, and increase education.

3. Augmented Reality

Augmented reality is a more versatile and practical version of virtual reality, as it does not fully immerse individuals in an experience. Augmented reality features interactive scenarios that enhance the real world with images and sounds that create an altered experience. The most common current applications of this overlay of digital images on the surrounding environment include the recent Pokémon Go fad or the additions on televised football in the U.S.

Augmented reality can impact many industries in useful ways. Airports are implementing augmented-reality guides to help people get through their checks and terminals as quickly and efficiently as possible. Retail and cosmetics are also using augmented reality to let customers test products, and furniture stores are using this mode to lay out new interior design options.

The possibilities for augmented reality in the future revolve around mobile applications and health care solutions. Careers in mobile app development and design will be abundant, and information technology professionals can put their expertise to use in these interactive experiences.

4. Blockchain Data

Blockchain data, like the new cryptocurrency Bitcoin, is a secure method that will continue to grow in popularity and use in 2019. This system allows you to input additional data without changing, replacing, or deleting anything. In the influx of shared data systems like cloud storage and resources, protecting original data without losing important information is crucial.

The authority of many parties keeps the data accounted for without turning over too much responsibility to certain employees or management staff. For transaction purposes, blockchain data offers a safe and straightforward way to do business with suppliers and customers. Private data is particularly secure with blockchain systems, and the medical and information technology industries can benefit equally from added protection.

5. Cyber-Privacy and Security

Shared company systems and the growth of the Internet leave a high amount of personal and company data at risk to breaches. Redesigned systems and new firewalls and gateways will be added to the services companies need to bolster their technology. Cybersecurity is a concentration of IT that will help secure clouds and improve the trust between businesses and their vendors.

6. Internet of Things

The Internet of Things (IoT) is an emerging movement of products with integrated Wi-Fi and network connectivity abilities. Cars, homes, appliances, and other products can now connect to the Internet, making activities around the home and on the road an enhanced experience. Use of IoT allows people to turn on music hands-free with a simple command, or lock and unlock their doors even from a distance.

Many of these functions are helping organizations in customer interaction, responses, confirmations, and payments. Remote collection of data assists companies the most. IoT almost acts like a digital personal assistant. The intelligent features of some of these IoT products can aid in many company procedures. Voice recognition and command responses will allow you to access stored data on cloud services.

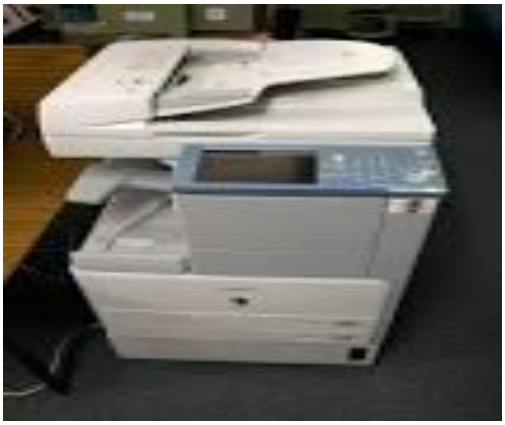
(https://www.vistacollege.edu/blog/careers/it/trends-in-information-technology-for-2019/)

2.2. MINIATURIZATION

- the trend to manufacture ever smaller mechanical, optical and electronic products and devices. Examples include miniaturization of mobile phones, computers and vehicle engine downsizing.
- In electronics, Moore's Law predicted that the number of transistors on an integrated circuit for minimum component cost doubles every 18 months. This enables processors to be built in smaller sizes

MULTIFUNCTIONAL MACHINES

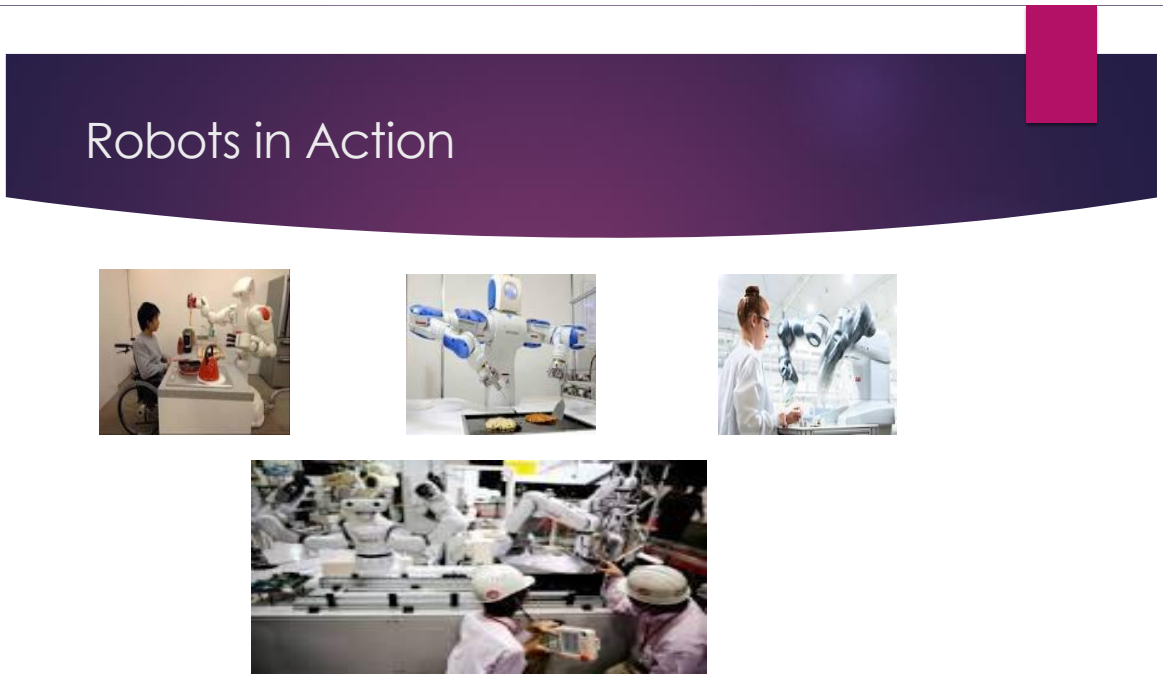
- An MFP (Multi-Function Product/ Printer/ Peripheral), multi-functional, all-in-one (AIO), or Multi-Function Device (MFD), is an office machine which incorporates the functionality of multiple devices in one



2.3 THE RISE OF ROBOTICS

- Robotics is a branch of engineering that involves the conception, design, manufacture, and operation of robots. This field overlaps with electronics, computer science, artificial intelligence, mechatronics, nanotechnology and bioengineering.
- Science-fiction author Isaac Asimov is often given credit for being the first person to use the term robotics in a short story composed in the 1940s. In the story, Asimov suggested three principles to guide the behavior of robots and smart machines. Asimov's Three Laws of Robotics, as they are called, have survived to the present:

    1. Robots must never harm human beings.
    2. Robots must follow instructions from humans without violating rule 1.
    3. Robots must protect themselves without violating the other rules.



LET’S ASSESS WHAT YOU HAVE LEARNED:

While emerging and converging information communication technologies promise radical changes in science and society, they also take away aspects of our lives such as our jobs and security, which will be replaced by Robotics. What are the things that robots cannot replace in humans, despite the rise of robotics?

CHAPTER 3. ICT-ENABLED INDUSTRY

Overview: Many ICT-enabled services are increasingly tradable as a result of technological advances in ICTs, combined with ongoing liberalization of trade and investment in services, and services activities are globalizing rapidly. These increasingly globalized service activities not only contribute to the development of the ICT sector but also more broadly to other business and service activities

Learning Objective:

At the of the Chapter, the student must be able to:

1. Design, implement and evaluate computer-based systems, processes, components, or programs to meet desired needs and requirements
2. Identify options for future job opportunities
3. Identify the different ways to have a sustainable professional career

3.1 BUSINESS PROCESS OUTSOURCING (BPO)

a. Business process outsourcing (BPO) is the contracting of a specific business task, such as payroll, human resources (HR) or accounting, to a third-party service provider. Usually, BPO is implemented as a cost-saving measure for tasks that a company requires but does not depend upon to maintain their position in the marketplace.

b. One of the most dynamic and fastest growing sectors in the Philippines is the Information Technology - Business Process Outsourcing (IT-BPO) Industry. The industry is composed of eight sub-sectors, namely, knowledge process outsourcing and back offices, animation, call centers, software development, game development, engineering design, and medical transcription. The IT-BPO industry plays a major role in the country's growth and development.

c. BPO Setups (Captive Markets and Offshoring/Third Party Outsourcing)
   - Third Party Outsourcing
     c.1 Project Based Outsourcing- primarily used for business activities with irregular frequencies or one-off projects. The usual costing method makes use of time and material costs as variable costs and the fixed costs
     c.2 Dedicated Development Center - primarily used in business cases when there are hanging requirements. In this specific model it could be used for some long-term goals for developing technology or software. This is preferred when resource requirements are lower in the outsourced country than the home country hence developing a comparative advantage. The customers (multinational firms) are charged for fixed fees, which are the wages of full-time employees

d. BPO Setups (Captive Markets and Offshoring/Third Party Outsourcing)
   - **Captive Markets**- preferred when core or crucial business activities are needed to be run at cheaper costs. The rationale for employing such a setup is to cater to long term strategic plans involving high managerial control. In this case there are two major ways of setting up a captive market and these are the DIY or 'Start From Scratch' model and the Build Operate Transfer model

e. BPO Setups (Captive Markets and Offshoring/Third Party Outsourcing)

- **Captive Markets : Start From Scratch Model**

  e.1 The usual flow is for the company to develop all its resources in the new designated area or country of operations.

  e.2 preferred by the companies that have high levels of market knowledge and analytics

- **Build Operate Transfer Model**

  e.3 the practice is to contact a 3rd party vendor in order to develop a contract in which the vendor is the one who develops the property, sources the employees and manages the BPO center for the first designated period or amount of time.

  e.4 preferred by companies that do not have any specialized expertise in the new country of operations hence needing a local partner or vendor to assist with market entry strategies

f. Trends in the Industry

- Better Information security
- Strategic balanced-shore outsourcing
- Booming Blogging and Social Media Outsourcing
- Popularity of cloud-based software

g. Issues concerning the industry in the Philippines

a. Health Issues - employees experience back and shoulder pains, due to the workstation setups and monitor levels, several have complained about experiencing throat irritations due to dealing with multiple calls a day coupled with a high stress work environment and concerns regarding the employees' hearing being damaged due to most of these workers being exposed to higher noise levels

b. Political Issues

- revision of Republic Act 7916 to include floors in buildings where BPO companies operates to be considered as special economic zones, exempting the companies from national and local taxes and only having to pay 5% of their gross income as tax
- approval of RA 7916, the establishment of the Philippine Economic Zone Authority(PEZA) which considered IT Parks as special economic zones, encouraged foreign investment in the industry by providing subsidies for infrastructure development and tax exemptions

c. Economic Issues

- the BPO industry is the fastest growing sector in the country and is expected to overtake OFW remittances in 2017
- the growth in the BPO industry has barely trickled down to most of the Philippine population
- the development of the country mainly because of the high unemployment and underemployment rates; the BPO industry was the fastest growing sector from 2005-2012 but only took in 1% of the labor force

3.2 MOBILE-BASED SERVICE INDUSTRY

Defined as those companies, which together enable the provision of telecommunication, information and entertainment services including voice, internet, SMS, text and other data services

- Mobile banking,
- economic development,
- delivery of health services,
- citizen empowerment and;
- greater access to media and education

3.3 E-SERVICES/E-GOVERNMENT

E-Government in the Philippines is envisioned to create "a digitally empowered and integrated government that provides responsive and transparent online citizen-centered services for a globally competitive Filipino nation."

- Efficient delivery of public services (Citizens)
- Places a premium on value-added, shared services, interoperability and the maximization of public resources (Government)
- Provides spaces for participation and fosters synergy in governance (Civil Society Organizations)
- Identifies policy and advocacy areas that need to be addressed in creating an environment necessary for fostering an integrated, interoperable and harmonized system of e-Governance (Policymakers)

LET'S ASSESS WHAT YOU HAVE LEARNED:

One of the most dynamic and fastest growing sectors in the Philippines is the Information Technology-Business Process Outsourcing (IT-BPO). Do you think that the BPO Industry contributes to the development of the ICT Sector and other business and service activities in our country?

CHAPTER 4. INTERNET CENSORSHIP AND FREEDOM OF EXPRESSION

Overview: Government may regulate, or **censor speech** if it has a compelling interest, is a public concern, or threatens national safety. ... On the other hand, the regulation of material on the **Internet would**, in fact, violate the First Amendment right to **free speech** and **expression**.

Learning Objective:

At the end of the Chapter, the student must be able to:

- Analyze and decide on boundaries between what is legal or not

4.0 Internet Censorship

Internet censorship is the control or suppression of what can be accessed, published, or viewed on the Internet enacted by regulators, or on their own initiative. Individuals and organizations may engage in self-censorship for moral, religious, or business reasons, to conform to societal norms, due to intimidation, or out of fear of legal or other consequences. The extent of Internet censorship varies on a country-to-country basis. While most democratic countries have moderate Internet censorship, other countries go as far as to limit the access of information such as news and suppress discussion among citizens.

Internet censorship also occurs in response to or in anticipation of events such as elections, protests, and riots. An example is the increased censorship due to the events of the Arab Spring. Other areas of censorship include copyrights, defamation, harassment, and obscene material. Internet Censorship in China known for having the most incredibly censored internets in the world. Internet Censorship in Philippines The Cybercrime Prevention Act of 2012, officially recorded as Republic Act No. 10175, is a law in the Philippines approved on September 12, 2012.

It aims to address legal issues concerning online interactions and the Internet in the Philippines. Among the cybercrime offenses included in the bill are cybersquatting, cybersex, child pornography, identity theft, illegal access to data and libel.

Internet censorship and content restrictions can be enacted through a number of different strategies which we describe below. Internet filtering normally refers to the technical approaches to control access to information on the Internet, as embodied in the first two of the four approaches described below.

1) TECHNICAL BLOCKING

There are three commonly used techniques to block access to Internet sites: IP blocking, DNS tampering, and URL blocking using a proxy. These techniques are used to block access to specific Web Pages, domains, or IP addresses. These methods are most frequently used where direct jurisdiction or control over websites are beyond the reach of authorities. Keyword blocking, which blocks access to websites based on the words found in URLs or blocks searches involving blacklisted terms, is a more advanced technique that a growing number of countries are employing. Filtering based on dynamic content analysis—effectively reading the content of requested websites—though theoretically possible, has not been observed in our research. Denial of service attacks produce the same end result as other technical blocking techniques—blocking access to certain websites—carried out through indirect means.

2) SEARCH RESULT REMOVALS

In several instances, companies that provide Internet search services cooperate with governments to omit illegal or undesirable websites from search results. Rather than blocking access to the targeted sites, this strategy makes finding the sites more difficult.

3) TAKE-DOWN

Where regulators have direct access to and legal jurisdiction over web content hosts, the simplest strategy is to demand the removal of websites with inappropriate or illegal content. In several countries, a cease and desist notice sent from one private party to another, with the threat of subsequent legal action, is enough to convince web hosts to take down websites with sensitive content. Where authorities have control of domain name servers, officials can deregister a domain that is hosting restricted content, making the website invisible to the browsers of users seeking to access the site.

4) INDUCED SELF-CENSORSHIP

Another common and effective strategy to limit exposure to Internet content is by encouraging self-censorship both in browsing habits and in choosing content to post online. This may take place through the threat of legal action, the promotion of social norms, or informal methods of intimidation. Arrest and detention related to Internet offenses, or on unrelated charges, have been used in many instances to induce compliance with Internet content restrictions. In many cases, the content restrictions are neither spoken nor written. The perception that the government is engaged in the surveillance and monitoring of Internet activity, whether accurate or not, provides another strong incentive to avoid posting material or visiting sites that might draw the attention of authorities.

The advantage of allowing internet censorship is that content which is violent, obscene, or dangerous can be immediately blocked. This protects children from inadvertently viewing content that could be scary or harmful to them, such as the murder and decapitation videos which have made their way to sites like Facebook and Twitter in recent years. The disadvantage is obvious: internet censorship is a restriction on a person's ability to view the content they wish to see, when they wish to see it. Here are some additional internet censorship pros and cons to discuss.

What Are the Pros of Internet Censorship?

1. It creates the chance to set common sense limits. There are some things that just aren't part of what a society would deem to be healthy. A simple search right now on an unfiltered public search can provide anyone with access to numerous videos that purport to show real murders in progress. High-profile cases, such as the murders of Alison Parker and Adam Ward, were broadcast on-air and then a first-person video of the event made its way through social circles afterwards. Restricting this content sets a common-sense limit on the content that van be viewed.

1. It limits access to harmful activities. There are dark areas of the internet where anything goes right now. Access to illicit drugs, sex trafficking, human trafficking, and child pornography can be accessed with relative ease by those who seek out such things. By restricting content that can be accessed, it limits the opportunities that predators can create to reach out to find new victims.

2. It could lessen the impact of identity theft. One of the fastest growing crimes in the world today is identity theft. NBC News reports that more US citizens were victims of identity theft in 2016 than any year before. More than 15.4 million reports of identity theft were compiled by Javelin Strategy and Research, which reflects a 16% increase in the total number of reports from 2015 figures. Restricting content that would allow identity information to be easily shared could lessen the impact that identity theft causes to a society.

3. It may provide a positive impact on national security. Although hacking will occur no matter what internet censorship laws may be in place, by creating internet censorship regulations with strict and mandatory penalties for a violation, it could become possible to reduce the number of hacking incidents that occur. That could have a positive impact on national security because the restrictions would possibly prevent alleged incidents like what occurred during the 2016 US Presidential election.

4. It stops fake news. Claims of fake news increased dramatically in 2017. Fake news websites promote false reports for money through clicks because readers think the news is real. Internet censorship would provide another level of discernment which could possibly stop divisive incidents that are based on events that never occurred.

What Are the Cons of Internet Censorship?

1. **Who watches the watchers?** Even if internet censorship is directly supervised and ethically maintained, someone somewhere is deciding on what is acceptable and what is not acceptable for society to see online. At some level, someone does not have anyone to whom they report regarding their censorship decisions. With that kind of power, one individual could influence society in whatever way they chose without consequence.

2. **It stops information**. Although fake information can be restricted through internet censorship, so can real information. According to the World Economic Forum, 27% of all internet users live in a country where someone has been arrested for content that they have shared, published, or simply liked on Facebook. 38 different countries made arrests based solely on social media posts in 2016.

3. **It is a costly process**. According to research from Darrell West, VP and Director of Governance Studies and the founding director of the Center for Technology Innovation at Brookings, internet shutdowns cost countries $2.4 billion in 2015. The decision to cut connectivity in Egypt came at a cost of $90 million. Censoring content is costly and it will come at the expense of taxpayers.

FREEDOM OF EXPRESSION

- Right to express one's ideas and opinions freely through speech, writing, and other forms of communication but without deliberately causing harm to others' character and/or reputation by false or misleading statements.
- According to the Universal Declaration of Human Rights, proclaimed in 1948, Everyone has the right to freedom of opinion and expression.
- This right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Freedom of expression is recurrently limited through tactics that include censorship, restrictive press legislation and harassment of journalists, bloggers and others who voice their opinions, as well as crackdowns on religious minorities.

The right to freedom of expression is a fundamental human right, which is shown as a corollary of human dignity, representing a necessary foundation for the survival of the state. Therefore, it should be defended by all the citizens and protected by certain authorities. It is also closely related to freedom of religion and freedom of the press.

As it is a core to the definition of freedom, the importance of free speech as a basic and valuable characteristic cannot be underestimated.
At an individual level, freedom of expression is the key to the development and fulfilment of every person.

- People can gain an understanding of their surroundings and the wider world by exchanging ideas and information freely with others. This makes them more confident and more able to plan their lives and to work. Sharing ideas can enhance productivity at the workplace, not to mention that it fosters social relationships

At a national level, freedom of expression is necessary for good government and therefore for economic and social progress.

- Free debate about new legislation helps ensure that the eventual law has the support of the population, making it more likely to be respected;
- If people can speak their minds without fear, and the media are allowed to report what is being said, the government can become aware of any concerns and address them.
- Free debate about and between political parties exposes their strengths and weaknesses, as a result media scrutiny of the government and the opposition helps expose corruption or other improprieties and prevents a culture of dishonesty.

Although you have freedom of expression, you also have a duty to behave responsibly and to respect other people's rights.
Public authorities may restrict this right if they can show that their action is lawful, necessary and proportionate in order to:

- protect national security, territorial integrity (the borders of the state) or public safety
- prevent disorder or crime
- protect health or morals
- protect the rights and reputations of other people
- prevent the disclosure of information received in confidence
- maintain the authority and impartiality of judges
- An authority may be allowed to restrict your freedom of expression if, for example, you express views that encourage racial or religious hatred.

Using digital technologies for freedom of expression

Technically, people can have global access to information. The amount of information available to the masses is incomprehensible. At the same time, Internet security and monopolistic structures have created new dangers to freedom of speech and access to information.

1. **Social media** - is the general term used to describe the plethora of web-based applications that allow people to create, share and exchange information, opinions and ideas in virtual communities. Social media use Internet and mobile technologies to create interactive platforms

where individuals and communities share, co-create, discuss and modify user-generated content. however, it is necessary to be mindful of the dangers of using social media as well.

- Social media conjure up many different types of data security and access to information issues. These platforms are run by businesses after all. Media projects can use social media to reach current and new audiences. They can also use it to collect and collate data, to crowdsource information and to develop platforms for discussions on certain topics. Social media can also be used as advocacy and lobbying tools to raise awareness amongst the general public of a specific issue.

2. **YouTube/Soundcloud** - are online websites that enable people to upload and share videos and audio for free. A variety of businesses, artists, experts and organizations use them to disseminate ideas and information to a wide audience.

3. **Mobile Phones** - have been around for decades and new advancements in smartphones support a variety of additional services such as business, news, social and game applications and photography.

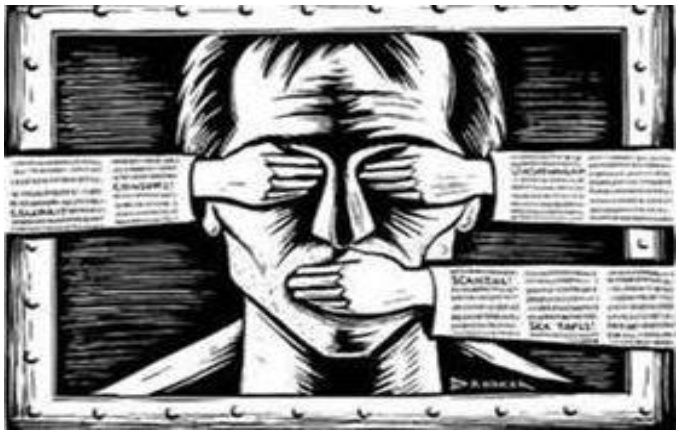
4. **Online Website** - may not be new but the way that they are being used to reach wider demographics and new audiences can be considered innovative. Being online gives organizations and businesses a platform to represent their work to the world.

5. **Tablet/computers** - are compact mobile computers that are interactive with touchscreens and have capabilities such as inbuilt cameras and microphones that make them ideal for roving reporters and journalists who are capturing stories on the go.

Advantages

- Allows individuals to express their opinions
- Less corruption
- Freedom from hunger
- A healthier society
- Respect for environment
- Respect for fundamental human rights
- Improve national security
- Make the political system more democratic
- Make the government more efficient
- Lead to better decision-making
- Help the economy become more efficient
- Individuals will receive better treatment from institutions

This black and white picture depicts a middle-aged man with his eyes and mouth covered. The artist creates an atmosphere of sadness, distress and pain, representative of the inability of the man to open his horizons, to follow his dreams. At the first glance we immediately realize how lucky we are: we have the power to speak, to think, to argue.



Conclusion:

Freedom of expression, the right to express one's ideas and opinions freely through speech, writing, and other forms of communication, has developed towards progress over the years. However, there is still a long path to tread to type it as universal.

Some experts have been asking where our freedom stops. In my opinion, there is no freedom which is absolute and unlimited. The exercise of the right to freedom of expression carries with its duties and responsibilities; it may be subject to formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society.

"Proclaim the truth and do not be silent through fear." - Catherine of Siena

4.1 WEBSITE CONTENT FILTRATION

Need of filtering:

1. Safe access to the internet
2. For business
3. Protect children for unsuitable contents

Content Filtering

- On the internet, content filtering is the use of a program to screen and exclude from access or availability web pages or e-mail that is deemed objectionable.
- Content filtering usually works by specifying character strings that, if matched, indicate undesirable content that is to be screened out.

Types of filtering

Filters can be implemented to many different ways. No solution provides complete coverage, so most companies deploy a mix of technologies to achieve the proper content control in line with their policies.

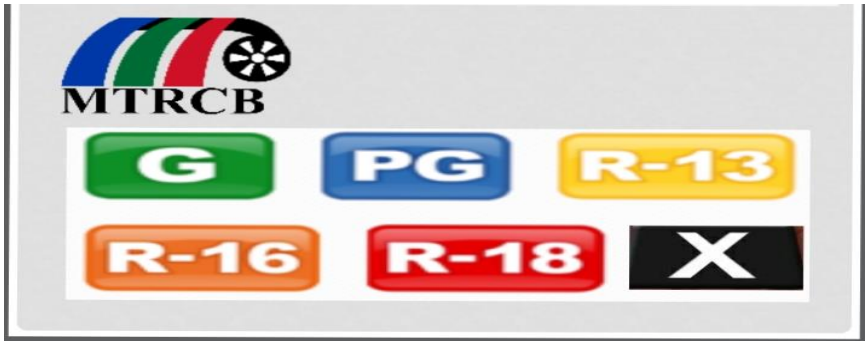
1. **Browser Based** Filters - It is the most lightweight solution to do content filtering, and is implemented via third party extensions.
   - Blocksi is the #1 rated extension for web & Youtube filtering, time management and trend analysis for Chrome and Chromebooks.

2. **E-Mail Filters** - E-mail filters set on information contained in the mail headers such as sender, and subject, and e-mail attachments to classify, accept or reject messages.

3. **Search-Engine Filters** - Many search engines, such as Google and Bing offer users the option of turning on a safety filter. When this safety filter is activated, it filters out the inappropriate links from all of the search result.

Problems with Filtering

It could be expected that allowed content would be blocked. If all pornographic content is to be blocked, other content with a resemblance in features will also be blocked e.g. sex education, medical information etc.



4.2 CENSORSHIP VS REGULATION

Television and Films - The Movie and Television Review and Classification Board (MTRCB) – is a Philippine government agency under the Office of the President of the Philippines that is responsible for the classification and review of television programs, movies and home videos.

- The government agency can classify a movie or television program an X-rating which forbids the material from being shown to the public due to issues such as excessive obscenity.

Films Description

G (General Patronage) – Viewers of all ages are admitted.
PG (Parental Guidance) – Viewers below 13 years old must be accompanied by a parent or a supervising adult.
R-13 – Only viewers who are 13 years old and above can be admitted.
R-16 – Only viewers who are 16 years old and above can be admitted.
R-18 – Only viewers who are 18 years old and above can be admitted.
X – "X – rated" films are not suitable for public execution.

LET'S ASSESS WHAT YOU HAVE LEARNED:

The right to freely express one's ideas and opinions is known as freedom of expression. Where do you think our FREEDOM stops?

CHAPTER 5. SEX AND TECHNOLOGY

Overview: Modern technology is almost inseparable from our daily lives. However, criminals often take advantage of vulnerabilities in cyber security to commit crimes through the use of computer technology. If members of the public lack security awareness of computer network security, they can easily fall prey to online swindlers. Police appeal to the public to be vigilant and thereby avoid potential technology crime hazards. Whilst using computer as the medium, technology crime is not that much different from traditional crime. Various common types of technology crime are listed here.

Learning Objective:

At the end of the Chapter, the student must be able to:

- Realize that crimes are also committed in the Cyberworld;
- Develop a sense of responsibility.

5.1 CHILD PORNOGRAPHY

Child pornography is a form of child sexual exploitation. The law defines child pornography as any visual depiction of sexually explicit conduct involving a minor (persons less than 18 years old). Images of child pornography are also referred to as child sexual abuse images.

The law prohibits the production, distribution, importation, reception, or possession of any image of child pornography.

The expansion of the Internet and advanced digital technology lies parallel to the explosion of the child pornography market. Child pornography images are readily available through virtually every Internet technology, including social networking websites, file-sharing sites, photo-sharing sites, gaming devices, and even mobile apps. Child pornography offenders can also connect on Internet forums and networks to share their interests, desires, and experiences abusing children, in addition to selling, sharing, and trading images.

These online communities have promoted communication and collaboration between child pornography offenders, thereby fostering a larger relationship premised on a shared sexual interest in children. This has the effect of eroding the shame that typically would accompany this behavior, as well as desensitizing those involved to the physical and psychological damage caused to the child victims. For this reason, online communities attract and encourage new individuals to join them in the sexual exploitation of children.

The methods many offenders use to evade law enforcement detection have also become increasingly sophisticated. Purveyors of child pornography continue to use various encryption techniques and anonymous networks on “The Dark Internet”, attempting to hide their amassed collections of illicit child abuse images. Several sophisticated online criminal organizations have even written security Material s to ensure that their members follow preferred security protocols and encryption techniques in an attempt to evade law enforcement and facilitate the sexual abuse of children. (https://www.justice.gov/criminal-ceos/child-pornography)

5.2 VIRTUAL PROSTITUTION AND CYBER SEX

Virtual sex is sexual activity where two or more people - or one person and a virtual character - gather together via some form of communications equipment to arouse each other, often by the means of transmitting sexually explicit messages. (Wikipedia)

Virtual Prostitution is an activity in which one engages in sexual activity with another person, whom neither have ever seen/met in real life before. Usually the two met online.

(https://www.urbandictionary.com/define.php?term=Virtual%20Prostitution)

Using the Internet to access prostitution-related information and engage in virtual prostitution empowers men to sexually exploit women and children. The combined experience of using high tech computer hardware and software, finding a supportive community in the Internet, and having a sexual experience (masturbating to pornography, live sex shows and writing about prostitution) is reinforcing and empowering. Pedophile behaviors are reinforced in that the perpetrator acts in an environment with no social rules, and with minimal chance of being held accountable.

Prostitution is not a victimless crime. Each sex act, whether online or not, is a violation of women's dignity and bodily integrity.

The technology is part of the excitement. The newest, fastest becomes the sexiest and enables the best sexual experiences online. Using the Internet to access pornography leads to an escalation of accessing, collecting and using pornography. The cycle continues.

(https://prezi.com/votfz9hmi0qp/virtual-prostitution/)

5.3 CYBER SEX

Cybersex can be defines as those sexual acts that are derived from surfing electronic media sites that would titillate the sexual mind and the at satisfies the erotic needs of an individual. These sites might be on Websites, Chat-rooms with web cams, streaming video materials, live sex shows and / or SMS messages.

TYPES OF CYBERSEX USER

a. Group 1: Recreational Users – Appropriate

This group pf cybersex users are able to occasionally explore sex on the internet without problems. They might use cybersex to enhance their sexual experiences. They are able to enjoy intimate sexual relationships in the real world and have a healthy attitude to sexuality. So, although they are seeking sexual gratification online, it is considered appropriate and not pathological. As online dating is increasingly common, they may use website to meet potential sexual partners, but other than meeting and communicating with partners online, they are as appropriate and respectful in these relationships as people who enjoy meeting potential dates in person.

b. Group 2: Recreational Users - Inappropriate

Like appropriate recreational users, this group of cybersex users can also access internet sex without compulsive use but may use this material inappropriately. This could include sexting

or showing sexual images to other people for amusement or shock value, causing unintentional embarrassment. Such users do not keep their activities secret and may otherwise have a healthy attitude towards sexuality and relationship.

c. Group 3: Problematic Users – Discovery Group

This group has not had any past problems with online other sexual behavior. They may be using the internet as a way to explore sexuality in a way that normal life has not offered them. Examples of problematic users in the discovery group are people who compulsively visit adult dating sites in the hope of meeting a partner, while avoiding real-life opportunities to meet people; or people who use the internet in an attempt to meet an underage partnet for sex, despite no prior history of doing so. They may also be using dating sites to meet multiple partners in a manipulative or dishonest way.

d. Group 4: Problematic Users – Predisposed Group

This group includes people who may have a history of fantasizing about sexual acting out, but who have never done it until accessing internet-based sexual material. They might have thought about going to strip clubs or seeing prostitutes for sex, but not taken any action to do so, perhaps for fear of recognition or other consequences. Their use may be regular but not excessive, although attention is taken away from real relationships, work life may suffer, or infidelity can occur.

e. Group 5: Problematic Users – Lifelong Sexually Compulsive Group

People in this group are at the extreme end if the continuum of sexual problems. Their sexual acting out occurs with or without access to the internet—the oneline world simply adds another avenue to explore sexually inappropriate material. These cybersex users may access pornography frequently, as part of an ongoing pattern of excessive secual behavior. They may also engage in predatory behavior in seeking out and exploiting vulnerable partners.

Although not all cybersex users engage in problematic internet use, all take the risk that their use may become problematic. One difficulty with the online world of sex is that while users are detached from their surroundings, sexually aroused, and surfing the net, they may be exposed to images they would never seek out normally. This can lead to exploring illicit sexual material in a way that was never intended, sometimes with dire legal and relationship consequences.

Why cybersex?

- Websites can be accessed anytime, anywhere with anonymity
- If not participating in cybersex with a known partner, people can portray a new identity
- There are no consequences like sexually transmitted diseases or pregnancy
- Can experiment sexually without anyone knowing their true identity
- Can portray a different version of themselves that's a different gender or age

When can cybersex be harmful?

a. Use cybersex as a means to:
   - Cope
   - Handle boredom, anxiety, and other powerful feelings
   - Feel important, wanted, and powerful

b. Spend multiple hours away from their work and family
c. Online at times when the household is asleep -> lack of concentration at work or school
d. Unable to stop themselves from engaging
e. Social relationships may decline as the person spends numerous hours engaging in cybersex
f. May not be able to refrain from accessing the materials in the workplace (Help Guide, 2014)
g. May grow anxious and restless if unable to access computer (Sexual Recovery Institute, 2014)

5.4 <u>ONLINE RELATIONSHIPS</u> - is a relationship between people who have met online and in many cases know each other only via the Internet.

ADVANTAGES:

- can immediately focus on people with similar interest, beliefs, age and other important criteria.
- Meaningful dating can be done at a distance, even in other countries.
- Allows you to expand your options outside you social circle.

DISADVANTAGES:

- Scammers
- Data Shared is Permanent
- Misleading Form of Attraction
- Distance is a Barrier

EXAMPLES OF ONLINE DATING APP / SITE:

- PROFUOUNDLY
- NEARGROUP
- TINDER
- OMEGLE

LET'S ASSESS WHAT YOU HAVE LEARNED:

Each sex act, whether online or not, is a violation of women's dignity and bodily integrity and because of technology, such acts can be easily derived from surfing electronic media sites. How can you, being a responsible student and citizen, avoid a potential technology crime such as cybersex, virtual prostitution and the like?

CHAPTER 6. TECHNOLOGY AND PRIVACY

Overview: Most people know by now social media isn't free – it's paid for with the collection of its users' sometimes-sensitive information. Your GPS system keeps track of your movements and your smart TV or webcam can watch you. Almost all the information these devices collect can be sold to companies or used by government and law enforcement to keep tabs or gather evidence. At the same time, we use technology so frequently as a society because it allows us to do things faster and with much less efforts.

Learning Objectives:

At the end of the Chapter, the student must be able to:

- Understand professional, ethical, legal, security and social issues and responsibilities in the utilization of information technology

6.1 IDENTITY THEFT - also known as identity fraud, is a crime in which an imposter obtains key pieces of personally identifiable information (PII), such as Social Security or driver's license numbers, to impersonate someone else.

The taken information can be used to run up debt purchasing credit, goods and services in the name of the victim or to provide the thief with false credentials. In rare cases, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

There are many **different examples of identity theft**, including:

1. **Financial identity theft.** This is the most common type of identity theft. Financial identity theft seeks economic benefits by using a stolen identity.

2. **Tax-related identity theft**. In this type of exploit, the criminal files a false tax return with the Internal Revenue Service (IRS). Done by using a stolen Social Security number.

3. **Medical identity theft.** Where, the thief steals information like health insurance member numbers, to receive medical services. The victim's health insurance provider may get the fraudulent bills. This will be reflected in the victim's account as services they received.

    - **Criminal identity theft**. In this example, a person under arrest gives stolen identity information to the police. Criminals sometimes back this up with a containing stolen credentials. If this type of exploit is successful, the victim is charged instead of the thief.

    - **Child identity theft.** In this exploit, a child's Social Security number is misused to apply for government benefits, opening bank accounts and other services. Children's information is often sought after by criminals because the damage may go unnoticed for a long time.

    - **Senior identity theft.** This type of exploit targets people over the age of 60. Because senior citizens are often identified as theft targets, it is especially

important for this seniors to stay on top of the evolving methods thieves use to steal information.

- **Identity cloning for concealment.** In this type of exploit, a thief impersonates someone else in order to hide from law enforcement or creditors. Because this type isn't explicitly financially motivated, it's harder to track, and there often isn't a paper trail for law enforcement to follow.

- **Synthetic identity theft.** In this type of exploit, a thief partially or completely fabricates an identity by combining different pieces of PII from different sources. For example, the thief may combine one stolen Social Security number with an unrelated birthdate. Usually, this type of theft is difficult to track because the activities of the thief are recorded files that do not belong to a real person.

Identity theft techniques

Although an identity thief might hack into a database to obtain personal information, experts say it's more likely the thief will obtain information by using social engineering techniques. These techniques include the following:

1. **Mail theft.** This is stealing credit card bills and junk mail directly from a victim's mailbox or from public mailboxes on the street.
2. **Dumpster diving.** Retrieving personal paperwork and discarded mail from trash dumpsters is an easy way for an identity thief to get information. Recipients of preapproved credit card applications often discard them without shredding them first, which greatly increases the risk of credit card theft.

3. **Shoulder surfing.** This happens when the thief gleans information as the victim fills out personal information on a form, enter a passcode on a keypad or provide a credit card number over the telephone.

4. **Phishing.** This involves using email to trick people into offering up their personal information. Phishing emails may contain attachments bearing malware designed to steal personal data or links to fraudulent websites where people are prompted to enter their information.

MONITORING

Employers are justifiably concerned about threats to and in the workplace, such as theft of property, breaches of data security, identity theft, viewing of pornography, inappropriate and/or offensive behavior, violence, drug use, and others. They seek to minimize these risks, and that often requires monitoring employees at work. Employers might also be concerned about the productivity loss resulting from employees using office technology for personal matters while on the job. At the same time, however, organizations must balance the valid business interests of the company with employees' reasonable expectations of privacy.

Magnifying ethical and legal questions in the area of privacy is the availability of new technology that lets employers track all employee Internet, e-mail, social media, and telephone use.

(https://opentextbc.ca/businessethicsopenstax/chapter/privacy-in-the-workplace/)

INTRUSION/INVASION OF PRIVACY

Invasion of privacy is a legal term. It is used to describe a circumstance where an individual or organization knowingly intrudes upon a person. The intrusion occurs when the person has a reasonable expectation of privacy, such as in a bathroom or locker room.

An invasion of privacy is considered to be a tort. A tort is a wrongful act that causes injury or loss to someone resulting in legal responsibility for the wrongful act.

a. Deception

One type of invasion of privacy, in some states, is called deception. Deception occurs when an employer collects information he claims is for one reason but uses it for another reason, which could result in the employee's termination.

An example of deception is if an employer sets up a blood drive and tells employees that donations will be used to aid a local blood bank. The blood drawn from employees is tested for drugs as part of the process. The employer could be accused of deception if he uses the drug results as a reason to terminate employees if employees did not consent to being drug tested.

b. Violation of Confidentiality

A second type of invasion of privacy is violating an employee's confidentiality. This occurs when information given in confidence is then given to a third party.

For example, an employee has a wife and children but decides to leave his insurance policy to an unrelated female coworker. If the human resources manager reveals this confidential information to another employee, it is considered an invasion of privacy.

c. Intrusion & Misappropriation

A third type of invasion of privacy is intrusion. This occurs in business when an employer intrudes in an employee's private life. What you do in the privacy of your own home is your business and an employer may not interfere with that because you have a reasonable expectation of privacy.

(https://study.com/academy/lesson/what-is-invasion-of-privacy-definition-examples.html)

LET'S ASSESS WHAT YOU HAVE LEARNED:

We are currently living in the "information age," which can be defined as a period in which most economic activities are based on information. What impact do you believe technology has on people's private lives?

CHAPTER 7. INFORMATION WARFARE

Overview: into their political intentions and decision making process. **Information warfare** opens new avenues for the conduct of politico-military operations. On the low level of the conflict spectrum, covert intrusion into an opponent's command and control system may provide unique insight

Learning Objective:

At the end of the Chapter, the student must be able to:

- Understand professional, ethical, legal, security and social issues and responsibilities in the utilization of information technology

INFORMATION WARFARE – is defined as "action as taken to achieve information superiority by affecting an adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks.

Information Warfare (IW) – is a concept involving the battlespace use and management of information and communication technology (ICT) in pursuit of a competitive advantage over an opponent. IW is the manipulation of information trusted by a target without the target's awareness, so that the target will make decisions against their interest but in the interest of the one conducting information warfare. As a result, it is not clear when information warfare begins, ends, and how strong or destructive it is. Information warfare may involve collection of tactical information, assurance(s) that one's own information is valid, spreading of propaganda or disinformation to demoralize or manipulate the enemy and the public, undermining the quality of opposing force information and denial of information-collection opportunities to opposing forces. Information warfare is closely linked to psychological warfare.

Information warfare can take many forms:

- Television, internet and radio transmission(s) can be jammed.
- Television, internet and radio transmission(s) can be hijacked for a disinformation campaign.
- Logistics networks can be disabled.
- Enemy communications networks can be disabled or spoofed, especially online social community in modern days.
- Stock exchange transactions can be sabotaged, either with electronic intervention, by leaking sensitive information or by placing disinformation.
- The use of drones and other surveillance robots or webcams.
- Communication management

Weapons of Information Warfare

a. Information Collection

Information collection is included as part of information warfare because "[t]he information revolution implies the rise of a mode of warfare in which… the side that knows more… will enjoy decisive advantages,". The idea is that the more information one has, the higher his/her situational awareness, which leads to better battle plans and, hopefully, better outcomes. According to Singh, "[t]ill recently, knowing your position and that of the friendly forces was itself a huge task. Precision position locating technologies such as navigation based on the Global Positioning System (GPS)

has eased those problems to a large extent. Knowing the position of the enemy has also been made possible to a degree through employment of renaissance and surveillance technologies." In information warfare, information collection is much less dangerous and much more complete because these technologies can be used to infiltrate situations and gather accurate information with minimal loss of fidelity.

b. Information Transport

Collecting a large amount of comprehensive information is certainly good practice, but collection is little value if the information sits in a storage facility, unused. As such, the ability to transport information into the hands of those who need it, in a timely manner, is another essential aspect of information warfare. The tools used in this domain are not exactly weapons, but rather civilian technologies put to use in military situations. The most important of these tools is communication infrastructure, composed of networks of computers, router, telephone lines, fiber optic cable, telephones, televisions, radios, and other data transport technologies and protocols. Without these technologies, the ability to transport information in the real-time fashion required by today's standards would be impossible.

c. Information Protection

One of the most broadly agreed upon aspects of information warfare is the need to minimize the amount of information to which your opponent has access. A large part of this is protecting the information you have from capture by the other side. The weapons used to protect the security of our information fall in two classes. First are those technologies that physically protect our vital data storage facilities, computers, and transport mechanisms, including bomb and bullet proof casings and intrusion prevention mechanisms such as locks and fingerprint scans. Second, and perhaps more important, are technologies that prevent bits from being seen and intercepted by the enemy. This certainly includes basic computer security technologies such as passwords, as well as more sophisticated technologies like encryption.

d. Information Manipulation

Information manipulation in the context of information warfare is the alteration of information with intent to distort the opponent's picture of reality. This can be done using a number of technologies, including computer software for editing text, graphics, video, audio, and other information transport forms. Design of the manipulated data is usually done manually so those in command have control over what picture is being presented to the enemy, but the aforementioned technologies are commonly used to make the physical manipulation process faster once content has been decided

e. Information Disturbance, Degradation and Denial

The final aspects of information warfare, according to our earlier definition, are disturbance, degradation, and denial. All three techniques are means to the same general end – preventing the enemy from getting complete, correct information. Because of their similarity, many of the same weapons are used to achieve one or more of the goals. As such, it makes sense to discuss them together. Some of the more popular weapons used to wage these types of information warfare are spoofing, noise introduction, jamming, and overloading.

Types of Information Warfare

1. Command and Control Warfare

The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions.

2. Intelligence-Based Warfare

Intelligence-Based Warfare is a unique concept, you wouldn't know what parts of the network to destroy in order to disrupt decision making if you didn't have good intelligence.

3. Electronic Warfare

Electronic Warfare are those techniques that enhance, degrade or intercept the flow of information electronically. Any military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum.

4. Psychological Warfare

The term used "to denote any action which is practiced mainly by psychological methods with the aim of evoking a planned psychological reaction in other people". Psychological Warfare are planned operations to convey selected information and indicators to audiences to influence their emotions, motives, objective reasoning and ultimately the behavior of organizations, groups, and individuals.

5. Hacker Warfare

Hacker Warfare is probably the most familiar portion of Information Warfare for most of us. This type of warfare is also known as Computer Network Operations (CNO) and is often portrayed in movies and headlines. One of the biggest areas of IW where the military and civilian lines get mixed up and you start to see military attacks on civilian companies to gain a desired effect on an enemy.

6. Economic Information Warfare

It is defined as channeling or blocking information to pursue economic dominance. EIW can be defined as the economic impact of Information Warfare on country or company. There are two areas of EIW, **information blockade and information imperialism**. A nation or company would cut-off the targeted countries access to outside information. This blockade would cripple the economy of the targeted nation.

7. Cyberwarfare

It is the use of information systems against the virtual personas of individuals or groups. It is the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.

7.1 CYBER ESPIONAGE

Espionage, according to Merriam-Webster, is "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company."

Take this into the cyber world, and the spies are armies of nefarious hackers from around the globe who use cyber warfare for economic, political, or military gain. These deliberately recruited and highly valued cybercriminals have the technical know-how to shut down anything from government infrastructures to financial systems or utility resources. They have influenced

the outcome of political elections, created havoc at international events, and helped companies succeed or fail.

Many of these attackers use advance persistent threats (APTs) as their modus operandi to stealthily enter networks or systems and remain undetected for years and years. (https://www.carbonblack.com/definitions/what-is-cyber-espionage/)

Cyberespionage involves the use of information and communication technology (ICT) by individuals, groups, or businesses for some economic benefit or personal gain (Maras, 2016; for more information on cyberespionage for economic benefit, see Cybercrime Instructional Material 11 on Cyber-Enabled Intellectual Property Crime). **Cyberespionage** may also be perpetrated by government actors, state-sponsored or state-directed groups, or others acting on behalf of a government, seeking to gain unauthorized access to systems and data in an effort to collect intelligence on their targets in order to enhance their own country's national security, economic competitiveness, and/or military strength (Maras, 2016). While espionage is not a new phenomenon, ICT have enabled illicit intelligence collection efforts directed and/or orchestrated by other countries at an unprecedented speed, frequency, intensity, and scale (Fidler, 2012), as well as a reduction of risks associated with committing espionage (i.e., being caught by the country that is being targeted by the collection efforts) (Ziolkowski, 2013).
https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html

7.2 INTELLIGENCE GATHERING

An intelligence gathering is collecting of information about a particular entity for the benefit of another through the use of mor than one, inter-related source.

Intelligence Gathering Discipline

1. Human Intelligence (HUMINT) – is intelligence gathered by means of interpersonal contract, as opposed to the more technical intelligence gathering disciplines. Can provide several kinds of information. It can provide observations during travel or other events from travelers, refugees, escaped friendly POWs, etc. It can provide date on things about which the subject has specific knowledge, which can be another human subject or, in the case of defectors and spies, sensitive information to which they had access. Finally, it can provide information on interpersonal relationship and network of internet.

2. Geospatial Intelligence (GEOINT) – is intelligence about human activity on earth derived from the exploitation and analysis of imagery and geospatial information that describes, assess and visually depicts physical features and geographically referenced activities on the earth.

3. Measurement and Signature Intelligence (MASINT) – is a technical branch of intelligence gathering which serves to detect, track, identify or describe the signature (distinctive characteristics) of fixed or dynamic target sources. This often includes radar intelligence, acoustic intelligence, nuclear intelligence and chemical and biological intelligence. MASINT is defined as scientific and technical intelligence derived from the analysis of data from sensing instruments for the purpose of identifying any distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification.

4. Open-source Intelligence (OSINT) – is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt,

publicly available source (as opposed to covert or clandestine sources). It is not related to open-source software or public intelligence.

OSINT under one name or another has been around for hundred of years. With the advent of instant communication and rapid information transfer, a great deal of actionable and predictive intelligence can now be obtained from public, unclassified sources.

5. Signals Intelligence (SIGINT) – is intelligence-gathering by interception of signals, whether communications between people)communication intelligence – abbreviate to COMINT) or from electronic signals not directly used in communications (electronic intelligence – abbreviated to ELINT) Signals intelligence is a subset of intelligence collection management.

As sensitive information is often encrypted, signals intelligence in turn involves the use of cryptanalysis to decipher the messages. Traffic analysis – the study of who is signaling whom and in what quantity - is also used to derive information.

6. Technical Intelligence (TECHINT) – is intelligence about weapons and equipment used by the armed forces of foreign nations (often referred to as foreign material). The related term, scientific and technical intelligence, addresses information collected on the strategic (i.e. national) level.

Technical intelligence is intended primarily to allow the armed forces to avoid technological surprise. Knowledge of the characteristics and capabilities or enemy weapons allows nations to develop effective countermeasures for them. Occasionally, armed forces adopt technology developed by foreign nations.

7. Cyber Intelligence /Digital Network Intelligence (CYBINT/DNINT) – is gathered from cyberspace or interconnected technology.

8. Financial Intelligence (FININT) – is the gathering of information about the financial affairs of entities of interest, to understand their nature and capabilities, and predict their intentions. Generally, the term applies in the context of law enforcement and related activities.

One of the main purposes of financial intelligence is to identify financial transactions that may involve tax evasion, money laundering or some other criminal activity. FININT may also be involved in identifying financing of criminal and terrorist organizations.

LET'S ASSESS WHAT YOU HAVE LEARNED:

With the guarantee of a promising career move, your superior directed you to obtain highly sensitive information from a competitor company. Would you accept or decline the offer, and why?

CHAPTER 8. E-HEALTH

OVERVIEW: e-Health is an emerging field in the intersection of medical informatics, public **health** and business, referring to **health** services and information delivered or enhanced through the Internet and related technologies.

Learning Objectives:

At the end of the Chapter, the student must be able to:

- Identify and analyze user needs and take them into account in the selection, creation, evaluation and administration of computer-based systems

e-Health – the term characterized not only a technical development , but also a state-of-mind, a way of thinking an attitude, and commitment for networked, global thinking, to improve a healthcare locally, regionally and worldwide by using information and communication technology. (Journal of Medical Internet Research)

The cost effective and secure of information and communication technologies in support of the health and health-related, health surveillance and health education, knowledge and research. (World Health Organization WHO)

8.1 TELEMEDICINE

Telemedicine is the practice of medicine using technology to deliver care at a distance. A physician in one location uses a telecommunications infrastructure to deliver care to a patient at a distant site.

Telehealth refers broadly to electronic and telecommunications technologies and services used to provide care and services at-a-distance.

WHAT'S THE DIFFERENCE?

Telehealth is different from telemedicine in that it refers to a broader scope of remote health care services than telemedicine. **Telemedicine** refers specifically to remote clinical services, while telehealth can refer to remote non-clinical services.

https://www.aafp.org/media-center/kits/telemedicine-and-telehealth.html

TYPES OF TELEMEDICINE

1. Remote Patient Monitoring

Also known as telemonitoring, remote patient monitoring allows patients with chronic diseases to be monitored in their homes through the use of mobile medical devices that collect data about blood sugar levels, blood pressure and other vital signs. Remote caregivers can review the data instantly.

2. Store-and-Forwards

Also known as asynchronous telemedicine. Store-and-Forward telemedicine allows provides to share patient information such as lab results, with physical at another location.

3. Inter-active Telemedicine

Allows physicians and patients to communicate real-time. Such sessions can be conducted in the patient's home or in nearby medical facility and include telephone conversation of the use of video conferencing software that complies with Health Insurance Portability and Accounting Act Regulations.

ADVANTAGES OF TELEMEDICINE:

1. Convenience – Patients do have to take away from work for an appointment. There is also travel time or associated expenses, such as paying for gas of child care.

1. Increased Access – Patients in rural areas can obtain specialty services more easily. Patients who live in underserved areas have increase accessed primary, dental and mental healthcare.
2. Reduced cancellations or no-shows – Because of its convenience, telemedicine can reduce the number of cancellations or no-shows. Providers can reach out prior to or at the appointment time if the patient forgot about the appointment.

3. Encourage Healthy Lifestyle choices – allows providers to encourage their patients' healthy lifestyle choices, such as smoking cessation.

DIS-ADVANTAGES OF TELEMEDICINE

a. Inability to prescribe medications – many states generally do not allow online prescribing (not to be confused with e-prescribing) without an established relationship between the physician and patient.

b. Technical Training and Equipment – provides need to be trained on how to use telemedicine equipment. There are also the associated costs of the equipment, such as integrated telemedicine carts and encounter management software, to consider. The start-up cost of implementing telemedicine may be especially prohibited to rural facilities.

c. Licensing Issues – certain states may required providers who practice telemedicine across state lines have a valid license in the state where the patients is located.

8.2 VIRTUAL THERAPY

Virtual therapy is therapy that takes place via the phone, an app, a video chat, or even a virtual reality device. These virtual therapy options allow people to seek treatment in the comfort of their own home, without having to travel to see a therapist in person.

TYPES OF VIRTUAL THERAPY THROUGH ELECTORNIC DEVICE

Virtual therapy is a type of telemedicine. It includes any treatment that a person seeks through an electronic device.

- talking to a practitioner via videoconferencing software
- using an app to access therapy
- phone- and email-based therapies, such as when a physical therapist suggests specific exercises via email

- the use of online devices to assess clients or patients remotely — for instance, when a speech therapist uses online tools to measure progress

TYPES OF VIRTUAL THERAPHY

In theory, any treatment that does not require physical contact or laboratory testing can work on a virtual platform. The most prevalent types of virtual therapy include:

1. Virtual psychotherapy - sometimes called telemental health or telepsychology, treats people with mental health issues, relationship or sexual health problems, or significant stress via video chat, email, phone, text messaging, or email.

In most virtual psychotherapy sessions, a licensed therapist provides traditional therapy through a new platform. A client might talk about their emotions, seek insight on their relationships, and ask for help implementing lifestyle changes.

A newer form of **virtual psychotherapy** uses apps or coaching to improve mental health. This approach is not a form of traditional therapy because a person does not get care from a licensed practitioner. Instead, they might monitor their own symptoms over time, get virtual coaching from a bot, or receive daily mental health tips.

2. Virtual physical therapy - offers traditional care but in an online or phone-based setting. A physical therapist might discuss recent symptoms, recommend exercises, or administer screenings.

In some cases, a therapist might ask a client to perform exercises and then use a camera to evaluate their form and progress.

Some physical therapy apps complement therapy by offering additional exercises or allowing a client to track their progress between sessions. A person can use these apps alongside virtual or in-person therapy.

3. Virtual speech therapy - can treat a range of speech disorders, such as a stutter, aphasia from a stroke, or pronunciation difficulties.

In a virtual session, a therapist may evaluate a person's speech, offer them strategies for correcting speech issues, or help them practice new speech patterns. An emerging form of virtual speech therapy uses bots in place of real people to improve speech.

Virtual speech therapy apps are also available to help people work toward their speech goals between sessions or track speech changes over time.

4. Virtual occupational therapy - helps people master specific life skills. People often use it in conjunction with other types of treatment. For example, a person with speech issues resulting from a stroke might choose speech therapy, then use occupational therapy to help them master the motor skills necessary to use a speech assistive device.

In **virtual occupational therapy**, a therapist offers coaching, tips, and feedback on techniques on a virtual platform, such as via video chat. Some forms of virtual occupational therapy may also use virtual reality to mimic real-world situations that the individual might face.

BENEFITS AND DISADVANTAGES

Benefits

a. Virtual therapy is relatively new, and researchers have not thoroughly tested every type of treatment. However, preliminary research suggests that it could be effective.

For example, a 2020 study of virtual physical therapy following knee surgery found that virtual therapy offered similar benefits to in-person treatment. It also significantly lowered costs.

The authors of a 2017 systematic review also suggested that telemental health services provide a quality of care and outcomes similar to those of traditional mental healthcare.

Some other benefits of virtual therapy include:

- **Increased access to care**: People who have physical disabilities, are geographically isolated, or do not have time to drive to therapy can access treatment with virtual options.
- **More privacy**: Well-managed virtual therapy means that a person can get care in the privacy of their own home, without having to sit in a waiting room or interact with other clients.
- **Cost savings**: Virtual therapy may cost less. The overheads may be lower for the therapist, particularly if they switch to an exclusively online model of care.
- **Client satisfaction**: Most research on satisfaction following virtual therapy suggests that clients are at least as satisfied with it as they are with traditional care. For some people, seeking virtual care may be less stressful, greatly increasing satisfaction.

Disadvantages

Some drawbacks of virtual therapy include:

- **Data concerns**: If a therapist chooses the wrong platform or does not encrypt therapy sessions, a third party might violate a client's privacy. If a client seeks care on a public network or leaves their computer unlocked, their colleagues or housemates may be able to view their sessions.
- **Relationship concerns**: Depending on the modality the client chooses, it may be harder to form a trusting relationship with the therapist. For instance, email-based therapy removes body language and voice tone cues, potentially causing communication issues.
- **Technological limitations**: Slow networks, low quality video, and chat delays can make therapy more difficult.
- **Technological expertise and philosophy**: People who are not comfortable with technology may feel less comfortable with or more anxious about virtual treatment.

https://www.medicalnewstoday.com/articles/virtual-therapy#types

LET'S ASSESS WHAT YOU HAVE LEARNED:

People are afraid to leave their homes as a result of the global pandemic, and even going to the hospital is a concern. On the other hand, we were introduced to e-Health and Telemedicine as a result of this. Do you believe this method is effective and can be used even after the virus has been eradicated?

CHAPTER 9. ONLINE CRIMES

Overview: Cyber crimes are criminal offenses committed via the Internet or otherwise aided by various forms of computer technology, such as the use of online social networks to bully others or sending sexually explicit digital photos with a smart phone. But while cyber crime is a relatively new phenomenon, many of the same offenses that can be committed with a computer or smart phone, including theft or child pornography, were committed in person prior to the computer age.

Learning Objective:

At the end of the Chapter, the student must be able to:

- Understand professional, ethical, legal, security and social issues and responsibilities in the utilization of information technology

9.1 HACKING

Hacking - is seeking and exploiting weaknesses in a computer system or computer network, while **Cracking** is the more appropriate term for breaking into computers.

- refers to unauthorized intrusion into a computer or a network. The person engaged in hacking activities is known as hacker, This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.

TYPES OF HACKER

1. **WHITE HACKERS** – are the good guys of the hacker world. They typically have a strong IT security background, and may even be certified as an ethical hacker. They are sometimes called “penetration testers”.

2. **BLACK HAT HACKERS** – are the one’s you hear about in the news. They gain access to information from banks or other businesses and typically steal money, credit card information or proprietary data.

3. **GRAY HAT HACKERS** – are hackers who hack for their own purpose but don’t steal money or information, and typically don’t do it to help others.

4. **GREEN HAT HACKERS** – are the black hat hackers who are just starting out in the hacking world.

5. **RED HAT HACKERS** – are the vigilante who go after the black hat hackers using aggressive hacking methods.

HACKING TECHNIQUES

1. **VULNERABILITY SCANNER** – checks the computers on networks for known weaknesses.

2. **PASSWORD CRACKING** – the process of recovering passwords from data stored or transmitted by computer systems.

3. **PACKET SNIFFER** – applications that capture data packets in order to view data and passwords in transit over networks.

4. **SPOOFING ATTACK** – involves websites which falsify data by mimicking legitimate sites, and they are therefore treated as trusted sites by users or other programs.

5. **ROOT KIT** – represents a set of programs which work to subvert control of an operating system from legitimate operators.

6. **TROJAN HORSE** – serves as back door in a computer system to allow an intruder to gain access to the system later.

7. **VIRUSES** – self-replicating programs that spread by inserting copies of themselves into other executable code files or documents.

8. **KEY LOGGERS** – tools designed to record every keystroke on the affected machine for late retrieval.

9.2 SPAMMING

Spamming – to send (a message) indiscriminately to multiple mailing lists, individual, or newsgroups. The sending of multiple unsolicited e-mails or text messages, usually for marketing purposes.

These being said, here are **Five of the most common methods** spammers use and how you can effectively protect yourself against them.

- Comment **Spam**. Comment **spam** is awful. ...
- Trackback **Spam**. Trackbacks were created with the intention of being useful. ...
- Negative SEO Attack. ...
- Spiders, Bots and DDoS Attacks. ...
- E-mail **Spam**.

Spoofing - A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host

9.3 TECHNOLOGY-BASED TERRORISM

Terrorism, per se, is the calculated use of violence to create a general climate of fear in a population and thereby to bring about a particular political objective. Terrorism has been practiced by political organizations with both rightist and leftist objectives, by nationalistic and religious groups, by revolutionaries, and even by state institutions such as armies, intelligence services, and police.

Cyber-terrorism is the intimidation or coercion of a government or organization to advance an individual's or group's political or social objectives by launching computer-based attacks against computers, networks, and the information stored on them. Such attacks could be

accomplished by the sending of a virus or worm or through the launching of denial-of-service attack.

9.4 ONLINE FRAUD - is a type of **cybercrime** **fraud** or deception which makes use of the Internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance.[1] Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace. It is, however, differentiated from **theft** since, in this case, the victim voluntarily and knowingly provides the information, money or property to the perpetrator. It is also distinguished by the way it involves temporally and spatially separated offenders.

COMMON TYPES OF ONLINE FRAUD OR INTERNET SCAMS

a. **Identity Theft**. Using **malware** or computer intrusion techniques, cybercriminals steal personally identifiable information to assume someone else's identity.
b. **Credit Card Fraud**. Is when someone uses your **credit card** or **credit** account to make a purchase you didn't authorize. ... If you lose your **credit card** or have it stolen, it can be used to make purchases or other transactions, either in person or online.
c. **Auction Fraud**. Is defined by the Internet Crime Complaint Center as "**fraud** attributable to the misrepresentation of a product advertised for sale through an Internet **auction** site or the non- delivery of products purchased through an Internet **auction** site.
d. **Investment Fraud**. Involves the illegal sale or purported sale of financial instruments. The typical **investment fraud** schemes are characterized by offers of low- or no-risk **investments**, guaranteed returns, overly-consistent returns, complex strategies, or unregistered **securities**.
e. **Work-at-Home Scam. Home-based positions can be used as vehicles to carry out scams.** Phony employers pretend to have positions available that allow job seekers to work remotely. Instead, job seekers are tasked with facilitating questionable acts that are often illegal.
f. **Online Dating Scam**. Millions of people turn to online dating apps or social networking sites to meet someone. But instead of finding romance, many find a scammer trying to trick them into sending money.
g. **West African Scam.** - Nigerian scams involve someone overseas offering you a share in a large sum of money or a payment on the condition you help them to transfer money out of their country. While these scams originated in Nigeria, they now come from all over the world.

COMPUTER FRAUD – is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. The fraud will result in obtaining a benefit by:

- Altering computer is an unauthorized way (almost hacking)
- Altering, destroying, suppressing or stealing output usually to conceal unauthorized transactions
- Altering or deleting stored data
- Altering or misusing existing systems tools or software packages, or writing code for fraudulent purposes.

LET'S ASSESS WHAT YOU LEARNED:

Scammers, thieves, and saboteurs abound on the internet, making it a dangerous place to be. It's no surprise that cybercrime is on the rise, given the prevalence of smartphones and social media that track our every move. In the event of an online crime, how can you protect yourself?

CHAPTER 10. E-LIFESTYLE

Overview: E-lifestyle as patterns in which people live and spend their time and. money through Internet and **electronic** mediums. **E-lifestyle** has been associated with information and communication technology enabled products and services

Learning Objective:

At the end of the Chapter, the student must be able to:

- Integrate IT-based solutions into the user environment effectively
- Apply knowledge through the use of current technologies, skills, tools and practices

10.1 SMS ADDICTION

Leave it to psychologists to label yet another behavior an "addiction" — short message service (SMS), also commonly known as text messaging (or just plain "texting"). But let's back up a bit, because this is becoming commonplace with any new technology that seems to eat up people's time and attention.

In modern times, we can trace the desire to call certain behaviors without drugs "addictions" to the rise and popularity of coin-operated and home video games in the 1970s and 1980s. Parents watch their children move from spending hours in front of the television to spending hours in front of a video game (or going to the video arcade to escape their parents' watchful eye). The following pronouncements were not uncommon in the research literature at the time:

"It is suggested that the potential usefulness or harm of video games is still open to empirical validation; however, the potential for abuse is inherent" (Soper & Miller, 1983).

10.2 ONLINE AND NETWORK-BASED GAMING

Video game addiction, also known as gaming disorder or internet gaming disorder, is generally defined as the problematic, compulsive use of video games that results in significant impairment to an individual's ability to function in various life domains over a prolonged period of time.

These games are played online with other people and are especially addictive because they generally have no ending. Gamers with this type of addiction enjoy creating and temporarily becoming an online character. They often build relationships with other online players as an escape from reality.

1.3 ONLINE SHOPPING

Online shopping is a form of electronic commerce which allows consumers to directly buy goods or services from a seller over the **Internet** using a **web** browser. … When an **online store** is set up to enable businesses to buy from another businesses, the process is called business-to-business (B2B) **online shopping**.

ADVANTAGES OF ONLINE SHOPPING

1. Convenience of online shopping

Customers can purchase items from the comfort of their own homes or work place. Shopping is made easier and convenient for the customer through internet. It is also easy to cancel the transactions.

Top 6 reasons given by shoppers in buying through internet

a. Saves time and efforts.
b. Convenience of Shopping at home.
c. Wide variety / range of products are available.
d. Good discounts / lower prices.
e. Get detailed information of the product.
f. We can compare various models / brands.

2. No pressure shopping

Generally, in physical stores, the sales representatives try to influence the buyers to buy the product. There can be some kind of pressure, whereas the customers are not pressurized in any way in online stores.

3. Online shopping saves time

Customers do not have to stand in queues in cash counters to pay for the products that have been purchased by them. They can shop from their home or work place and do not have to spend time traveling. The customers can also look for the products that are required by them by entering the key words or using search engines.

4. Comparisons

Companies display the whole range of products offered by them to attract customers with different tastes and needs. This enables the buyers to choose from a variety of models after comparing the finish, features and price of the products on display, Sometimes, price comparisons are also available online.

5. Availability of online shop

The mall is open on 365 x 24 x 7. So, time does not act as a barrier, wherever the vendor and buyers are.

6. Online tracking

Online consumers can track the order status and delivery status tracking of shipping is also available.

7. Online shopping saves money

To attract customers to shop online, e-tailers and marketers offer discounts to the customers. Due to elimination of maintenance, real-estate cost, the retailers are able to sell the products with attractive discounts through online. Sometimes, large online shopping sites offer store comparison.

THE MAJOR DISADVANTAGES OF ONLINE SHOPPING ARE AS FOLLOWS.

1. Delay in delivery

Long duration and lack of proper inventory management result in delays in shipment. Though the duration of selecting, buying and paying for an online product may not take more than

15 minutes; the delivery of the product to customer' s doorstep takes about 1-3 weeks. This frustrates the customer and prevents them from shopping online.

2. Lack of significant discounts in online shops

Physical stores offer discounts to customers and attract them so this makes it difficult for e-tailers to compete with the offline platforms.

3. Lack of touch and feel of merchandise in online shopping

Lack of touch-feel-try creates concerns over the quality of the product on offer. Online shopping is not quite suitable for clothes as the customers cannot try them on.

4. Lack of interactivity in online shopping

Physical stores allow price negotiations between buyers and the seller. The show room sales attendant representatives provide personal attention to customers and help them in purchasing goods. Certain online shopping mart offers service to talk to a sales representative,

5. Lack of shopping experience

The traditional shopping exercise provides lot of fun in the form of show-room atmosphere, smart sales attendants, scent and sounds that cannot be experienced through a website. Indians generally enjoy shopping. Consumers look forward to it as an opportunity to go out and shop.

6. Lack of close examination in online shopping

A customer has to buy a product without seeing actually how it looks like. Customers may click and buy some product that is not really required by them. The electronic images of a product are sometimes misleading. The colour, appearance in real may not match with the electronic images.

People like to visit physical stores and prefer to have close examination of good, though it consumes time. The electronic images vary from physical appearance when people buy goods based on electronic images.

7. Frauds in online shopping

Sometimes, there is disappearance of shopping site itself. In addition to above, the online payments are not much secured. So, it is essential for e-marketers and retailers to pay attention to this issue to boost the growth of e-commerce. The rate of cyber crimes has been increasing and customers' credit card details and bank details have been misused which raise privacy issues.

10.4 BLOGGING, SOCIAL NETWORKS AND PERSONAL WEBSITES

A **blog** is a discussion or informational website published on the World Wide Web consisting of discrete, often informal diary-style text entries. Posts are typically displayed in reverse chronological order, so that the most recent post appears first, at the top of the web page. Wikipedia

The word **blog** is actually a shortened form of its original name, "weblog." The content of blogs varies significantly. For example, travel blogs may feature many pictures with few written

passages, while political blogs may weigh in with wordy takes on the news of the day. The popularity of YouTube and similar sites also gave rise to video blogging, or "vlogging."

Blogging refers to writing, photography, and other media that's self-published online. Blogging started as an opportunity for individuals to write diary-style entries, but it has since been incorporated into websites for many businesses.

Blogging vs. Websites

Blogs	Websites
Updated frequently	Largely evergreen content
Allows for reader engagement	One-way communication

Some people are confused over what constitutes a blog over a website. Part of the confusion stems from the fact that many businesses use both, usually by adding a blog section to the company website. However, there are **two features of a blog** that set it apart from a traditional website.

First, blogs are updated frequently. Whether it's a mommy blog in which a woman shares adventures in parenting, a food blog sharing new recipes, or a business providing updates to its services, blogs have new content added several times a week. Websites might occasionally have new information, but for the most part, they offer static information that rarely changes.

Secondly, blogs allow for reader engagement. Blogs and social media accounts often go hand-in-hand because they serve a similar purpose of connecting an audience with each other and the content creator. Some websites may incorporate features that allow for conversation, but generally speaking, a blog allows for more conversation and interaction than a traditional website does.

https://www.thebalancesmb.com/blogging-what-is-it-1794405

SOCIAL NETWORKS

Is a web site that creates an online community of Internet users that enables members to break down barriers created by time, distance and cultural difference.

Social networking web sites allow people to interact with others online by sharing opinions, insights, information, interests and experiences. Members of an online social network may use the site to interact with friends, family members and colleagues – people they already know – but they may also make use of the site to develop new personal relationships.

PERSONAL WEBSITES

Personal web pages are world wide **web pages** created by an individual to contain content of a **personal** nature rather than content pertaining to a company, organization or institution.

Resumes are boring. Career experts tell you to make your resume a one-page, size 11 Time New Roman document printed with black ink with no pictures. Seriously? How are you supposed to represent — and **differentiate** – yourself with that? Plus, your resume becomes static

and outdated the moment you hand it to someone. You can't update resumes you've already given out – you have to make new copies.

That's why you need to create a personal website. A website is the **complete opposite** of a resume. Everything bad about resumes can be fixed simply by having a website. I'd go as far as to say that **not** having a website is like shooting yourself in the foot – it's that useful.

Reasons Why You Need to Make a Personal Website

a. **A website isn't static; it's dynamic**. **It's ever-changing.** The moment you accomplish something, you can add it to your website. When you complete a project, you can put it in your portfolio for all to see. You don't need to print new copies of it and send it out to your contacts over and over; you just update it. People can continually come back and see what you're up to.

b. **Having a website makes you more findable.** If all you have is a resume, you have to go out and hand it to people to get your name out. If someone wanted to look you up on the internet and you didn't have a website, all they might get is a Facebook or Twitter profile.

   However, if you have a website, you can be found by a much wider audience *and* control what it is they see first. This is key for establishing your **personal brand** and for highlighting your accomplishments.

   I've been offered jobs, met clients for my web design work, and gotten interviews simply because I have a website. If I didn't take the time to create one, I'm confident that I wouldn't have been found. **Make sure you can be found!**

c. **Not many people have one.** Personal websites may be more common in 2020 than they were ten years ago, but the vast majority of students and job seekers are still relying on resumes and job search websites.

   Succeeding today requires that you make yourself **stand out,** and having a website can help you do that. It shows that you've taken the time to learn how to do something fairly technical, and it shows that you have some skills other people don't have.

d. **You gain some new skills that can be very useful in the future.** Learning how to build a website involves a number of different skills, especially if you get into customizing and optimizing things. Even if you're not looking for a job in a tech field, having these skills can give you a leg up.

   Say you're applying for a job in advertising. If you can tell the interviewer that you're not only a great marketer, but that you also have knowledge of the web, you become a **much more attractive candidate.**

10.5 HOME-BASED AND MOBILE OFFICES

What are the differences between working from home versus working in an office? Let's compare them side-by-side to help you understand the unique advantages and disadvantages of each.

Research from Owl Labs suggests that approximately half of employees typically work from home at least once a week and a third work remote jobs full-time.

Many organizations have shifted their tools and systems for remote teams for the first time due to the COVID-19 pandemic. For employees and employers, **this is a major adjustment.**

a. Commuting

The average American worker spends at least 27 minutes on their daily commute to work, and it is getting worse. More than 14 million people spend an hour or more traveling to work," according to NPR.

That's a lot of time you can save by becoming a telecommuter! Telecommuting is another way to say working remotely or from home by making full use of the internet, email, and phone.

However, some folks enjoy waking up early, getting ready, and having the separation of home and the office. This is why many folks who work remotely still opt to go to a coffee shop or a coworking space.

The bottom line is people hate commuting. Work-life balance continues to surge on the importance meter for modern-day employees. Companies that don't recognize this are missing a huge opportunity to adopt work from home strategies that benefit their workforce.

A poll posted by CEO of Product Hunt, Ryan Hoover, suggests that most people would take a pay cut if it gave them the ability to work remotely. Perks like infinite vacation time, free food, and 401k weren't as important when compared to the benefits of working remotely.

b. Communication

According to research from our 2020 State of Business Communication Report, face-to-face communication is the most preferred communication method by employees.

Not counting video conferencing, face-to-face communication is something you really only get in an office space. It's not only beneficial when planning for business, but it strengthens relationships and rapport with other employees. There's something about relationship-building that happens when you sit next to someone or bump into each other at the coffee machine.

Communication still happens when you're working remotely — it's just different. Face-to-face communication turns into video calls. Short conversations turn into Slack messages. Emails … well, those stay emails. Nobody escapes those!

One compelling advantage of working from home is the ability to work anywhere. You don't even need a laptop. With a full-featured business phone app, employees can make and receive calls, attend conference calls, message colleagues, and stay online using their iPhone or Android.

To improve communication for remote employees, we've seen many organizations require video conferencing over traditional phone calls when communicating with coworkers. Teams should have conference calls to align themselves with business goals. For fun, employees can even host online game nights to get to know each other outside of office life.

Some teams even rely on social media for communication. For example, Close.com says they use Snapchat internally for team building. It's a cool and clever way to use social media to stay connected while working remotely.

c. Flexibility

When working from an office, it's likely you have a set schedule. Your alarm goes off at the same time every day, you grab your morning coffee at 7:05 am, and you're at your desk by 9 am ready to work.

When it comes to working from home, it's a little different. You now have the flexibility to wake up when you choose and tailor your day to your needs. If your company is new to remote work, chances are they still want all employees working the traditional work hours of 9-to-5. With remote work, you can now wake up (a little) later, pick a time for lunch, and close your laptop when you want — for some, that's 4 pm, others it could be 7 pm.

As more companies adopt a remote-first policy, working hours will shift to fit the employee's schedule. This shift means more flexibility on when you start and end your day and where you work from. You should be able to work from anywhere that has a solid internet connection!

Many employees struggle to disconnect when working from home. Up to a third of employees say they struggle to balance work and home life when working remotely. It's easy to shut down your computer when you see fellow office workers start to pack up for the night, but when you're at home, those cues don't exist.

The option to freelance and take on side projects is another massive benefit that comes with working from home. The time you waste on commuting could be put toward taking on side projects or freelancing. It's far more lucrative than sitting through traffic jams!

("Working From Home vs. Working in an Office: Pros & Cons" by JEREMY BOUDINET https://www.nextiva.com/blog/working-from-home-vs-office.html)

LET'S ASSESS WHAT YOU HAVE LEARNED:

There are benefits and drawbacks to both online shopping and working from home. Given all of the possibilities, do you think your lifestyle will improve and become more worry-free?

CHAPTER 11. E-LEARNING AND DISTANCE EDUCATION

Overview: E-Learning can play a more support role of the teaching-learning activities organized in the class. As a result, a teacher may take its use for his better teaching and learning for his needed learning, e.g. they may use multimedia, internet and web services for their teaching and learning to enhance their classroom activities. **Distance learning** includes no in-person interaction between teachers and students.

Learning Objective:

At the end of the Chapter, the student must be able to:

- Recognize the need for and engage in planning self-learning and improving performance as a foundation for continuing professional development

11.1 COMPUTER-BASED TRAINING

Computer-based training (CBT) is any course of instruction whose primary means of delivery is a computer. A CBT course (sometimes called courseware) may be delivered via a software product installed on a single computer, through a corporate or educational intranet, or over the Internet as Web-based training. (https://whatis.techtarget.com/definition/computer-based-training-CBT)

Computer-Based Training (CBT) involves the use of a personal or networked computer for the delivery and access of training programs. CBT can be synchronous and asynchronous, as well as online, web-based, mobile, and distance learning. CBT is particularly useful when training learners on a specific computer application but can also be built to train learners on general knowledge or skills. The greatest disadvantage of CBT is that it is expensive to develop and deliver, especially for smaller groups of students. CBT can be more cost efficient when designed to train a larger number of students. (trainingindustry.com)

Computer-based training (CBT), often referred to as e-Learning, is education that is primarily administered using computers rather than an in-person instructor. CBT is typically delivered over the web using a training platform such as a learning management system (LMS).

Corporate training about topics such as security awareness and harassment often include difficult concepts for employees to adopt but using alternative training methods such as e-Learning can be a great way to make such an important and serious topic engaging and easy to comprehend. In fact, corporate e-Learning has grown by 900% in the past 16 years, and an Association for Talent and Development (ATD) report found that almost 90% of companies offer digital learning today.

BENEFITS OF CBT

1. Time, Money, and Savings

In-person training can come with many hidden costs, including travel, instructor fees, and employee productivity. Studies indicate that e-Learning has the potential to reduce overall training time by 40% – 60%. Reducing training time means more time for your employees to work on tasks that affect your organization's bottom line.

The best way to retain information learned during training is to regularly reinforce it. The cost of hiring someone to train employees and improve retention can be a large financial burden. E-Learning allows you to deploy courses to large or small groups of employees in a variety of time lengths to achieve optimal retention levels.

2. Higher Engagement & Retention Rates

E-Learning can increase a learner's retention rate by 25% to 60%. In contrast, the retention rate of face-to-face training can be much lower at 8% to 10%. With eLearning, employees and the organization have more control over the learning process. What's more, if they happen to forget something, they can revisit the material whenever they need to.

Additionally, new technology, such as virtual reality, provides engaging and immersive content that can be accessed by smartphones, thereby freeing users up from desktop computers. Role-playing can also give learners the opportunity to work through realistic situations with their coworkers. By handling the learning experience in these unique ways, employees can really get involved and engaged with training, making the content much more memorable.

3. Easier Scheduling and Deployment

Using CBT for corporate training efforts allows organizations to send out courses to large, small, or segmented groups for more specific training. Organizations can also send out reminders to ensure that training is not being forgotten.

4. Tracking Progress and Analytics

By deploying training through CBT, you'll be able to track the progress of your learners in the LMS. This will allow you to see when an employee started or finished their training. Some LMS platforms also allow you to see who has passed or failed a course, when users log in, the status of a course, etc. Seeing these types of analytics will allow you to drill down into which course topics need more attention and which topics employees are the most comfortable with.

5. Enhancing Competitiveness

In a survey by CertifyMe.net, almost 72% of organizations said that online learning is instrumental in enhancing their competitive edge. Organizations should consider offering incentives to individuals or departments in order to increase participation and create a positive mentality around required training.

6. Non-Threatening and Non-Judgmental

The immediate feedback of the computer-based training system allows employees to review portions of the material as frequently as needed, privately, and without feeling embarrassed by mistakes. Employees won't need to worry about taking quizzes slowly or staying on pace with other employees. (https://inspiredelearning.com/blog/benefits-of-computer-based-training-for-corporate-education/)

11.2 ONLINE EDUCATION/DISTANCE LEARNING

Online education is electronically supported **learning** that relies on the **Internet** for teacher/student interaction and the distribution of class materials." From this simple definition comes an almost infinite number of ways to teach and learn outside of traditional classrooms and away from college campuses

Benefits of Online Education

a. **Flexibility**. Students have the freedom to juggle their careers and school because they aren't tied down to a fixed schedule.
b. Reduced **Costs**. Online education can **cost** less due to a **variety** of reasons.
c. Networking Opportunities.
d. Documentation.
e. Increased Instructor - Student Time.
f. Access to Expertise.

These are the disadvantages of Online Education:

a. **Online** student feedback is limited.
b. **E-Learning** can cause social Isolation.
c. **E-Learning** requires strong self-motivation and time management skills.
d. Lack of communicational skill development in **online** students.
e. Cheating prevention during **online** assessments is complicated.

DISTANCE LEARNING

Distance education or **distance learning** is the **education** of students who may not always be physically present at a school. Traditionally, this usually involved correspondence courses wherein the student corresponded with the school via post. Today, it involves online **education**.

Advantages of Distance Learning

a. **You can take courses and learn from any university and/or instructor in the world**
b. **You make your own studying schedule** during the time the course is given
c. **You can get a degree from any university without leaving your home country** as long as you complete the required courses successfully
d. **You do not need to leave your employment position**, but can study whenever you have time and your job schedule allows it
e. **You can communicate and interact not only with the professor through virtual means, but also with other people around the world who are taking the same course as you**. This interaction can be done via email or chat rooms, and the students can be from different cultures or countries. This assists people in gaining more insight and expose themselves to different points of view that they might not have gained in a typical physical classroom with less diversity
f. Distance learning courses or degrees often **cost much less** than formally registering in a classroom at a physical university. As mentioned before, if you register in MOOCs, the courses are usually free of charge.

Disadvantages of Distance Learning

a. **Lack of physical social interaction** that is found in a typical, traditional classroom. Students can only engage and share opinions through virtual means in chatrooms or broadcasts, but are not able to physically interact with each other
b. **It does not fit all types of learners**. If you are someone who needs constant motivation and support from professors or instructors, then distance learning is not for you, since instructors are not always available to offer assistance in the same way that they would be in a traditional classroom

c. **Some courses required to complete a degree may not be available online**. Sometimes universities make many required courses online to give students a feel of their teaching methodologies, quality, and value. After you complete those courses, to get the degree you might be required to attend some classes in person. These classes will most likely be less affordable, or you will not be able to travel to the university to take them.
d. **You need to be technologically savvy**. If you are a person who is not as comfortable to working with technology, then distance learning will not suit you. Distance learning requires students to be able to operate with at least a minimum knowledge of different chat rooms, online examinations, and interaction, and many people do not feel comfortable if they do not even have physical material to study from.

LET'S ASSESS WHAT YOU HAVE LEARNED:

The days when distance and online education were just beginning to become more visible and accessible, piqued students' interest, are long gone. Online learning is almost as popular as on-campus learning these days. Which method of learning, face-to-face or e-learning, do you believe is more effective?