- Information and Communications Technology
  - **Contextualized Online Search and Research Skills**
  - **Current State of ICT Technologies**
    - WEB 2.0
      - Elements
      - Tools
      - History
      - Technologies
        - Adobo Flash
        - Microsoft Silverlight
        - JavaScript
        - Torrent
    - WEB 2.0 TO WEB 3.0
      - Expanded Definition
        - Ubiquitous Connectivity
        - Network Computing
        - Open Technologies
        - Open Identity
        - The Intelligent Web
      - Ubiquitus Computing
      - More Intelligent Web
        - Technologogical Convergence
          - Digital Convergence
          - Telecommunication Convergence
          - Media Convergence
    - Social and Assistive Media
      - Social Media
        - Microblogging
        - Social Curation
        - Wikis
      - Assistive Media
    - Educational Technology
      - Learning Management System
      - Social Media and Peer-to-Peer Platforms
      - Conferencing Applications
        - Online Meeting
        - Two-Way Audio
  - **Online Safety, Security, Ethics and Etiquette**
    - Your Online Data
      - Traditional Data
      - Internet of Things and Big Data
    - Online Security Threats and Attacks
      - Malicious Programs
        - Virus
        - Worms
        - Trojans
        - Bots
      - Phishing
    - Cybersecurity
    - Fighting Against Security Threats
      - Best Practices for Combating Malware Threats
        - Ensure that your operating system is up to date
        - Install an anti-virus software in your PC's
        - Firewall should always be enabled
        - Assure that the file to be downloaded is safe
        - Be cautious accepting or agreeing to prompts
      - Points to Ponder to Secure your Own Data
        - Use browsers in a private manner
        - You should take care when choosing a username or alias for your online identity
        - Choose your passwords wisely
        - Be careful when sharing documents, pictures, and other online resources via blogs or emails
        - Be aware of shoulder surfing
        - Verify data is encrypted
        - Be aware of social engineering
        - Use two-factor authentication if it is available
        - When connecting via Wi-Fi, log on to a secure network using WEP or WPA
    - Netiquette and Internet Chat Rooms
      - Email
      - Group Chat
      - Usenet

Information and Communications Technology

ICT is an acronym for Information and Communications Technology. A good way to think about ICT is to consider the use of technology, which enables individuals, businesses and organizations to use digital information. ICT covers any product that will store, retrieve, manipulate, transmit or receive information electronically in a digital form. This covers areas under education, banking, healthcare, government, business, and so many branches that we can think of.

1. Current State of ICT Technologies

Technology nowadays is mostly influenced by Internet access that is always under constant change due to the changing needs of consumers. The following represents the timeline of the web representation from Web 1.0 up until 3.0.

Timeline and Definitions

Web 1.0 is considered the foundation of web technology. The objective of Web 1.0 was to provide access to the Web itself, making the people to view and read the information. The key areas of interest centered on protocols such as HTTP, open standard markup languages such as HTML and XML, Internet access through ISPs, the first Web browsers, Web development platforms and tools, Web-centric software languages such as Java and Javascript, the creation of Web sites, the commercialization of the Web and Web business models, and the growth of key portals on the Web.

The infancy of Web 1.0 is the purpose of the birth of Web 2.0, known as the second generation of Internet-based services. Most of the Internet navigators are now able to perform modification of information, and interact with one another to share ideas and knowledge. This became the advent of social networking sites, wikis, communication tools, and folksonomies — that emphasize online collaboration and sharing among users. The purpose of this was to make sure that the site accessed by an Internet user is interactive. Another trend that has been a major factor in Web 2.0 is the emergence of the mobile Internet and mobile devices (including camera phones) as a major new platform driving the adoption and growth of the Web.

Web 3.0, the supposed third generation of Internet-based technological innovations, is referred to as ‘the intelligent Web’. At this instance, usage of semantic web, microformats, natural language search, data-mining, machine learning, recommendation agents, and artificial intelligence technologies — which emphasize machine-facilitated understanding of information in order to provide a more productive and intuitive user experience, became very common.

1.1. WEB 2.0

Web 2.0 is the current state of online technology as it compares with the early days of the Web, characterized by greater user interactivity and collaboration, more pervasive network connectivity and enhanced communication channels.

One of the most significant differences between Web 2.0 and the traditional World Wide Web (WWW, retroactively referred to as Web 1.0) is greater collaboration among Internet users, content providers and enterprises. Originally, data were posted on Web sites, and users simply viewed or downloaded the content. Increasingly, users have more input into the nature and scope of Web content and, in some cases, exert real-time control over it.1

The social nature of Web 2.0 is another major difference between it and the original, static Web. Increasingly, websites enable community-based input, interaction, content-sharing and collaboration. Types of social media sites and applications include forums, microblogging, social networking, social bookmarking, social curation, and wikis.

1.1.1. Elements

- **Online database** with adjustable content: There are websites that allow users to store information which can be retrieved at a later time. These sites also enable users to contribute, collaborate and edit site content. A good example of this is a wiki, which allows anyone to view and even modify information on the site.
- The increasing prevalence of **Software as a Service** (SaaS), web apps and cloud computing rather than locally-installed programs and services.
- **Mobile computing**, also known as nomadicity, the trend toward users connecting from wherever they may be. This trend is enabled by the proliferation of smartphones, tablets and other mobile devices in conjunction with readily accessible Wi-Fi networks.
- **Mash-ups**: Web pages or applications that integrate complementary elements from two or more sources.
- **Social networking**: The practice of expanding the number of one's business and/or social contacts by making connections through individuals.
- **Crowdfunding or Crowdsourcing**: Collaborative efforts based on the ability to reach large numbers of participants and their collective resources
- **User-generated content (UGC)**: Writing, images, audio and video content - among other possibilities - made freely available online by the individuals who create it.
- **Unified communications (UC)**: The integration of multiple forms of call and multimedia/cross-media message-management functions controlled by an individual user for both business and social purposes.
- **Social curation**: The collaborative sharing of content organized around one or more particular themes or topics. Social content curation sites include Reddit, Digg, Pinterest and Instagram.

1.1.2. Tools

- **Social media** are Web 2.0 tools allowing people to interact with one another exchange information, career interests, ideas, and pictures/videos in virtual communities and networks. A more detailed discussion of this is illustrated on Module 1.1.3.
- **Social bookmarking** is a user-defined taxonomy system for bookmarks. Such a taxonomy is sometimes called a folksonomy and the bookmarks are referred to as tags. Unlike storing bookmarks in a folder on your computer, tagged pages are stored on the Web and can be accessed from any computer.

This technology lets users organize their access to the web sites by storing the preferred sites that have been recently accessed, and then maybe accessed later on. Web sites dedicated to social bookmarking, such as Flickr and del.icio.us, provide users with a place to store, categorize, annotate and share favorite Web pages and files.

Unlike file sharing, social bookmarking does not save the resources themselves, merely bookmarks that reference them, i.e., a link to the bookmarked page. Descriptions may be added to these bookmarks in the form of metadata, so users may understand the content of the resource without first needing to download it for themselves.

- A **Podcast** is basically just an audio (or video) file. What distinguishes a podcast from other types of audio on the Internet is that a “podcaster” can solicit subscriptions from listeners, so that when new podcasts are released, they are automatically delivered, or fed, to a subscriber's computer or mobile device. Usually, the podcast features an audio show with new episodes that are fed to your computer either sporadically or at planned intervals, such as daily or weekly. This format encourages listeners to “subscribe.”2 Common podcast

applications include iTunes which can be used only for iOS devices, and Spotify, an application focusing on streaming service (streaming media is multimedia which allows a media file to be played before the entire file has been temporarily been transmitted.)

- **Educational tools**. There are two types of educational tools under Web 2.0. Electronic portfolios (also referred to as ePortfolios or Webfolios) are gaining recognition as a valuable tool for learners. It is practically a storage medium for individuals who wish to store learned information. Learning Management Systems (LMS), however, is faculty-centered type of application that is focused on providing tools for students to learn and be assessed with. LMS is owned by the institution to where it is currently being implemented while the ePortfolio is owned by the learner. As it is more popular and common today, LMS will be discussed further and will be the main topic on Module 1.1.4.1.

1.1.3. History

The foundational components of Web 2.0 are the advances enabled by Ajax and other applications such as RSS and Eclipse and the user empowerment that they support.

Darcy DiNucci, an information architecture consultant, coined the term “Web 2.0" in her 1999 article, "Fragmented Future”, indicating that the Web will be known to be a "transport mechanism, the ether through which interactivity happens. Darcy foresaw that the Web will be seen not only on personal computer units but in TV sets, car dashboards, mobile phones, and hand-held game machines as well. This was mostly observed when Palm Inc. started introducing their well known product - personal digital assistant, with Web access capability.

Tim O'Reilly is generally credited for popularizing the term, following a conference dealing with next-generation Web concepts and issues held by O'Reilly Media and MediaLive International in 2004. O'Reilly Media has subsequently been energetic about trying to copyright "Web 2.0" and holds an annual conference of the same name.

Tim O'Reilly and Dale Dougherty had a brief discussion to confer the changes experienced from Web 1.0 to Web 2.0, as summarized in Table 1.1.1.2a. For instance, the website for Encyclopedia Britannica online was popular before; most of the researchers tend to gather information from this site. In the new era, the attention of researchers are now focused on Wikipedia, as information are mostly updated by end users themselves.

1.1.4. Technologies

Adobe Flash

This is the plug-in on browsers used for delivering high-impact, rich Web content. Designs, animation, and application user interfaces are deployed immediately across all browsers and platforms, attracting and engaging users with a rich Web experience.1

Microsoft Silverlight
Silverlight is a powerful development tool for engaging on interactive user experiences for Web and mobile applications similar with Adobe Flash. This tool is a free plug-in that is based under the .NET framework and compatible with multiple browsers, devices and operating systems.2 It is different with Adobe Flash in terms of animation model used, compression formats, file size, platform capability, and so forth.

JavaScript
JavaScript is the programming language of HTML and the Web used to define the behavior of web pages.3 An instance of this is a new window being displayed after clicking an image, text shown in marquee mode (string of text displayed moving from left to right and vice versa), or a control being in and out of visibility. A more simple library used by programmers, which is jquery, is also used to ease up the content of code as it is already commercially free and available.

Torrent

Web 2.0 applications are often based on the decentralized download methodology that made torrent sites successful. A torrent is also a server, sharing the workload and making heavily demanded content more accessible that it would be in the centralized model where demand can lead to overwhelmed servers and pages. The media file is being downloaded from a swarm of distributed servers simultaneously instead of one centralized server, which makes it faster to download. All peers (downloaders and uploaders) may come and go, allowing the pieces to still be available for downloading, not like when you are directly downloading the file. Once done, a peer may still continue to upload, making him a seeder. The higher the number of seeders, the faster it is to download the file.

1.1.4.1. Adobo Flash

This is the plug-in on browsers used for delivering high-impact, rich Web content. Designs, animation, and application user interfaces are deployed immediately across all browsers and platforms, attracting and engaging users with a rich Web experience.

1.1.4.2. Microsoft Silverlight

Silverlight is a powerful development tool for engaging on interactive user experiences for Web and mobile applications similar with Adobe Flash. This tool is a free plug-in that is based under the .NET framework and compatible with multiple browsers, devices and operating systems.2 It is different with Adobe Flash in terms of animation model used, compression formats, file size, platform capability, and so forth.

1.1.4.3. JavaScript

JavaScript is the programming language of HTML and the Web used to define the behavior of web pages.3 An instance of this is a new window being displayed after clicking an image, text shown in marquee mode (string of text displayed moving from left to right and vice versa), or a control being in and out of visibility. A more simple library used by programmers, which is jquery, is also used to ease up the content of code as it is already commercially free and available.

1.1.4.4. Torrent

Web 2.0 applications are often based on the decentralized download methodology that made torrent sites successful. A torrent is also a server, sharing the workload and making heavily demanded content more accessible that it would be in the centralized model where demand can lead to overwhelmed servers and pages. The media file is being downloaded from a swarm of distributed servers simultaneously instead of one centralized server, which makes it faster to download. All peers (downloaders and uploaders) may come and go, allowing the pieces to still be available for downloading, not like when you are directly downloading the file. Once done, a peer may still continue to upload, making him a seeder. The higher the number of seeders, the faster it is to download the file.

1.2. WEB 2.0 TO WEB 3.0

Video: http://www.youtube.com/embed/bsNcjya56v8

Web enthusiasts believe that the Web 2.0 is just one phase that transformed World Wide Web into a newer and more established phase they call Web 3.0, also known as the Semantic Web.

Tim Berners-Lee, founder of WWW, suggested that the Web can still be improved as a whole in a more intuitive manner to serve the needs of the Internet users better. Berners-Lee noticed that users are unable to clearly choose the site that they need as multiple ones are being shown and indexed after entering the keywords in the search engine. He then suggests developers and authors, singly or in collaboration, to utilize self-descriptions to inform users of all suggested sites to lessen users' struggle in searching for the correct information. Web 3.0 will involve the publishing of web resources in languages intended for data (such as XML, RDF, OWL and XHTML) to supplement them with metadata that will allow software to analyze, classify and deliver content for more personal relevance. The Semantic Annotations for Web Services group at W3C is defining the specifications for the Web 3.0.

The evolution of Web 1.0 to 2.0 up until 3.0 which is where we are now is discussed in the link below. Click the image to play the video clip.

1.2.1. Expanded Definition

There are actually several major technology trends that are about to reach a new level of maturity at the same time. The simultaneous maturity of these trends is mutually reinforcing, and collectively driving the third-generation Web. From this broader perspective, Web 3.0 might be defined as a third-generation Web enabled by the convergence of several key emerging technology trends

1.2.1.1. Ubiquitous Connectivity

- Broadband adoption
- Mobile Internet access
- Mobile devices

1.2.1.2. Network Computing

- Software-as-a-service business models
- Web services interoperability
- Distributed computing (P2P, grid computing, hosted “cloud computing” server farms such as Amazon S3)

1.2.1.3. Open Technologies

- Open APIs and protocols
- Open data formats
- Open-source software platforms
- Open data (Creative Commons, Open Data License, etc.)

1.2.1.4. Open Identity

- Open identity (OpenID)
- Open reputation
- Portable identity and personal data (for example, the ability to port your user account and search history from one service to another)

1.2.1.5. The Intelligent Web

- Semantic Web technologies (RDF, OWL, SWRL, SPARQL, Semantic application platforms, and statement-based datastores such as triplestores, tuplestores and associative databases)
- Distributed databases — or what I call “The World Wide Database” (wide-area distributed database interoperability enabled by Semantic Web technologies)

1.2.2. Ubiquitus Computing

The model of Web 3.0’s machine-classified, data sharing world creates a basis for ubiquitous computing. Ubiquitous computing, also known as pervasive computing, is a scenario in which embedded processing in everyday objects enables intercommunication and unobtrusive data sharing throughout the user’s environment. The concept overlaps with that of the Internet of Things (IoT), in which almost any entity or object imaginable can be outfitted with a unique identifier (UID) and the ability to exchange data automatically. A modest example of this concept is a fridge that sends a grocery list to one’s smartphone.

The following defines clearly the elements involved in a pervasive computing system:

Information Context Aware
The ability to collect, metricize , monitor and platform machine to machine M2M, machine to human M2H telemetry across a wide range of structured, semi-structured and unstructured data

Situation Context Aware
The ability to create new physical and virtual environments with intelligence information an process context from the level large to the very small.

Internet of Things
The ability to multiplex and multiplicity of entities, assets and services spacing beyond the computing sphere into many other metasystems in social, commercial, organizational, biological and sustainability system

Pervasive computing relies on the convergence of wireless technologies, advanced electronics and the Internet. The goal of researchers working in pervasive computing is to create smart products that communicate unobtrusively. The products are connected to the Internet and the data they generate is easily available.

1.2.3. More Intelligent Web

The threshold of the third-generation Web will have been crossed in 2007. At this juncture, the focus of innovation will start to shift back from front-end improvements towards back-end infrastructure level upgrades to the Web. This cycle will continue for five to ten years, and will result in making the Web more connected, more open, and more intelligent. It will transform the Web from a network of separately siloed applications and content repositories to a more seamless and interoperable whole.

Because the focus of the third-generation Web is quite different from that of Web 2.0, this new generation of the Web probably does deserve its own name. In keeping with the naming convention established by labeling the second generation of the Web as Web 2.0, this third-generation of the Web could be called Web 3.0.

Technological Convergence

Technological convergence is the tendency that as technology changes, different technological systems sometimes evolve toward performing similar tasks. There are three common types of technological convergence:

1.2.3.1. Technologogical Convergence

1.2.3.1.1. Digital Convergence

Digital convergence refers to the convergence of four industries into one conglomerate, ITTCE (Information Technologies, Telecommunication, Consumer Electronics, and Entertainment). Previously separate technologies such as voice (and telephony features), data (and productivity applications), and video can now share resources and interact with each other synergistically. This is a way where new technological devices are being produced which are based from previous technologies performing the same tasks with advanced features.

1.2.3.1.2. Telecommunication Convergence

Telecommunications convergence, or network convergence, is the term used to describe emerging telecommunications technologies, and network architecture used to migrate multiple communications services into a single network. Specifically this involves the converging of previously distinct media such as telephony and data communications into common interfaces on single devices, such as most smart phones can make phone calls and search the web.

1.2.3.1.3. Media Convergence

Media convergence, in this instance, is defined as the interlinking of computing and other information technologies, media content, and communication networks that have arisen as the result of the evolution and popularization of the Internet as well as the activities, products and services that have emerged in the digital media space. Many experts view this as simply being the tip of the iceberg, as all facets of institutional activity and social life such as business, government, art, journalism, health, and education are increasingly being carried out in these digital media spaces across a growing network of information and communication technology devices.

1.3. Social and Assistive Media

1.3.1. Social Media

Social media is merely a collection of communication channels accessed through the Web and mobile applications with the purpose of allowing users to interact, collaborate, and exchange information, interests, ideas, and any visual representation with another user in a Web-based community.

1.3.1.1. Microblogging

Microblogging is a web service, which allows the subscriber to broadcast short messages to other subscribers of the service. This is a type of blog that lets users publish short text updates, the posts of which are termed microposts. Microposts can be made public on a Web site and/or distributed to a private group of subscribers

1.3.1.2. Social Curation

Social curation is collaborative online sharing of content organized around by an individual or number of people within the community. An alternate term, “content aggregation,” is sometimes proposed to mitigate how other discriminators disagree of the term curation as it is originally meant for the ones used in the field of arts. Among the oldest social curation sites are Digg and Reddit. Both of those sites allow users to suggest links to articles and allow other readers to give approval – on Digg, for example, by clicking a “thumbs up” icon. Higher approval ratings mean that a story will appear more prominently. Pinterest, on the other hand, is dedicated to images.

1.3.1.3. Wikis

Wikis are content management systems that provide collaborative modification of its content and structure directly from the web browser. Coined from a Hawaiian term which means quick, a wiki is run using wiki software, otherwise known as a wiki engine. In a typical wiki, text is written using a simplified markup language (known as "wiki markup"), and often edited with the help of a rich-text editor.

1.3.2. Assistive Media

Assistive media is an Internet-based audio reading service for people with reading impairments. This opens unique avenue of accessibility for said individuals with visual, cognitive, and communication disabilities. History dates back 1996 when David Erdody researched the availability of accessible audio-based reading materials for his father Kenneth Harmon Erdody who is suffering from diabetic retinopathy. Soon after, he discovered that less than 5% of U.S. publications were provided in an alternative audio format.

There is an existing site that allows one to access some of the available recordings (Click here (Links to an external site.)to access the site). The service offered by this site is open and free of charge, and there is no need for anyone to sign up to download the data. There is also no verification needed if the user is under reading disability.

1.4. Educational Technology

Research findings show that ICT can lead to improved student learning and better teaching methods. It has proven effective in contributing to universal access to education, equity in education, the delivery of quality learning and teaching, teachers’ professional development and more efficient education management, governance and administration.

Advantages of ICT for education

1. Through the use of ICT tools, mentors may be able to use images that will allow memory retention and boost of interest ensuring students' comprehension
2. Through the use of ICT tools, mentors may be able to explain complicated instructions and be able to easily access resources to knowledge being imparted to the students.
3. Through the use of ICT tools, mentors may be able to create an environment making the modules enjoyable, which could improve student attendance and concentration.

Disadvantages of ICT for education

1. The tools should be made available during the class. It would be a burden for the whole class if they will be unable to access the resources needed due to slow connection, loss of internet bandwidth, or sudden power outage.
2. The tools are expensive to afford - desktop/laptop units, licensed software, routers/switches, LAN cables, and so many more cost more than markers, whiteboards and board eraser.
3. Teachers should have a broad experience and knowledge when it comes to ICT tools usage.

1.4.1. Learning Management System

Learning Management System (LMS) is the most common option/format for teaching online. Click the image below to play the video clip, which summarizes the purpose of LMS.

https://youtu.be/FAsdtwj00Uo

Learning Management System functions solely as an online classroom where professors can:

- discuss modules online,
- upload reading materials,
- play educational videos and audio files,
- carry out learning activities,
- make announcements,
- assess and grade student work.

LMSs store and deliver materials developed in a variety of different formats — everything from MS Office documents to videos and third-party applications. They support synchronous (at the same time) and asynchronous (not at the same time) interactions between faculty and students and students and students. Online learning management systems can be hosted locally (i.e., kept on a server physically located at an educational institution) or remotely, “in the cloud” wherein the LMS company (Moodle Rooms or a Moodle partner, Desire to Learn, or Blackboard) manages all server-related issues. Wherever they reside, LMSs demand high-speed connectivity and strong bandwidth.1

Essentially all LMSs have “standard” or typical and uniform features, including:

- Analytics (with varying degrees of quality)
- Apps

- Assignment submission
- Discussion forum
- File upload/ download capacity
- Grading
- Instant messages
- Online calendar
- Online news and announcement (institution and course level)
- Online quiz
- Wiki
- Widgets that allow connections to social media

1.4.2. Social Media and Peer-to-Peer Platforms

Because Facebook is the most popular site on the World Wide Web (one of every seven minutes spent online is on Facebook), free social media networks can be an alternative to an LMS. Edmodo, for example, is a free educational social networking application. This type of application is used as an alternative to LMSs by universities and Ministries of Educations and schools all over the world because of the following reasons:

- **Cost**: It is free and available to everyone as long as one is connected to the Internet.
- **Educational focus**: Educational social networking apps are designed for teachers and students and online learning. It does not have or promote commercial content.
- **Less bandwidth intensive**: It supports low-bandwidth communications so students and instructors can carry on synchronous (real-time or live) and asynchronous (delayed) conversations without the need for a lot of bandwidth. Additionally, students or instructors with smart phones can access the Edmodo app and/or access the course via their phones, versus a computer.
- **Serves as an online classroom**: Edmodo makes for an excellent course site, allowing for readings to be housed in a library, the formation of small groups, discussions to be archived, third-party apps, and posting of photos and videos.
- **Familiar and easy to use**: Edmodo mimics Facebook in use and structure and should thus require very little training to use. It mimics an application with which, many instructors and students are familiar.

1.4.3. Conferencing Applications

1.4.3.1. Online Meeting

One alternative to the standard online course (via an LMS) or a social networking site is an online conferencing system that allows for webinars (seminars conducted via the web) and online meetings. Web conferences mimic the traditional lecture one finds in university or classroom--the instructor can lecture, share notes or a presentation and students can even virtually raise their hands and ask questions/communicate through voice or chat. The danger is that, unless university faculty are highly creative and determined to be different, this can really promote very instructor-lead, lecture-based instruction without any formal hands-on or simple practical application.

1.4.3.2. Two-Way Audio

A final option is to use two-way video for one-to-one coaching and tutoring (for example, Skype or Google Hangouts. This is an extraordinarily powerful form of online learning because it can provide intensive one-to-one (or one-to-many) instruction and support and make e-learning less impersonal and more “face-based.” And of course, seeing someone and talking with them one-on-one is so essential to developing rapport—and when online learners develop a rapport with their online instructor they are more likely to persist in an online course of study.

2. Online Safety, Security, Ethics and Etiquette

Almost all people surf the web to check their blogs and emails, download songs and videos, watch video clips, and so many other online activities. According to July 2016 statistics, there are already 3.4 BIllion Internet users worldwide.1 This means that there are so many people who are into browsing over the Internet worldwide. These users are prone to certain attacks, may it be one that cause damage or hacks your system to gather essential information.

Your Online and Offline Identify

As more time is spent online, your identity, both online and offline, can affect your life. Your offline identity is the person who your friends and family interact with on a daily basis at home, at school, or work. They know your personal information, such as your name, age, or where you live. Your online identity is who you are in cyberspace. Your online identity is how you present yourself to others online. This online identity should only reveal a limited amount of information about you. However, due to limited knowledge of what is happening around, most people neglect to consider securing the information via online.

Your online identity can also be considered as an actively constructed presentation of oneself. Although some people choose to use their real names online, some Internet users prefer to be anonymous, identifying themselves by means of pseudonyms, which reveal varying amounts of personally identifiable information. An online identity may even be determined by a user's relationship to a certain social group they are a part of online. Some can even be deceptive about their identity.

In some online contexts, including Internet forums, online chats, and massively multiplayer online role-playing games (MMORPGs), users can represent themselves visually by choosing an avatar, an icon-sized graphic image. Avatars are one-way users express their online identity. Through interaction with other users, an established online identity acquires a reputation, which enables other users to decide whether the identity is worthy of trust. Online identities are associated with users through authentication, which typically requires registration and logging in. Some websites also use the user's IP address or tracking cookies to identify users.2

A part of ICT learning is to make sure that individuals are aware of the online security threats and all possible measures to combat and prevent such attacks. The succeeding modules will be able to assist the students in such learning.

2.1. Your Online Data

Any information about you can be considered your data. This personal information can uniquely identify you as an individual. This data includes photos and messages that you exchange with your family and friends online. Other Information, such as name, social security number, date and place of birth, or mother‘s maiden name, is known by you and used to identify you.

2.1.1. Traditional Data

Corporate data include personnel information, intellectual properties, and financial data. Personnel information include application materials, payroll, offer letters, employee agreements, and any information used in making employment decisions. Intellectual property, such as patents, trademarks and new product plans, allows a business to gain economic advantage over its competitors. This intellectual property can be considered a trade secret; losing this information can be disastrous for the future of the company. The financial data, such as income statements, balance sheets, and cash flow statements of a company gives insight into the health of the company.

2.1.2. Internet of Things and Big Data

With the emergence of the Internet of Things (IoT), there is a lot more data to manage and secure. IoT is a large network of physical objects, such as sensors and equipment that extend beyond the traditional computer network. All these connections, plus the fact that we have expanded storage capacity and storage services through the Cloud and virtualization, lead to the exponential growth of data. This data has created a new area of interest in technology and business called “Big Data". With the velocity, volume, and variety of data generated by the IoT and the daily operations of business, the confidentiality, integrity and availability of this data is vital to the survival of the organization.

2.2. Online Security Threats and Attacks

2.2.1. Malicious Programs

We have been hearing worms, viruses, and Trojan horses, but we cannot usually distinguish one from the other. Most of the time, we even treat all malicious programs as viruses as this is the most common term people know; the terms are used interchangeably when they function unlikely from the other. Whatever their differences are, all of them are critical threats that can certainly damage our PC's or laptops.

Sources of threats

The following are the usual sources of threats and malware penetration:

- visiting sites that contains drive-by attack codes. A drive-by attack is a way where an exploit is being made which allows an attacker to gather information from the user or embedding a malware into the system as he is accessing the site. These sites may be accessed via an advertisement or a link sent to the via user
- downloading malicious software disguised as keygens, cracks, and patches
- downloading files via peer-to-peer networks (for example, torrents).
- downloading attachments from emails sent especially from unknown sources
- replying to emails involving your credentials such as credit card numbers, social security numbers, and few other things
- installing software applications with bugs, glitches and vulnerabilities
- plugging in removable media containing malicious programs

Common Effects of Malware

Damage from malware varies from causing minor irritation (such as browser popup ads), to stealing confidential information or money, destroying data, and compromising and/or entirely disabling systems and networks. The following specifically enumerates the list of possible effects of malware attacks:

- slowing down your operating system, your Internet speed or the speed of your applications.
- unexpected pop-ups appearing on the system; sometimes, they come bundled with other concealed malware threats, and which could be more destructive for our systems.
- system crashes frequently or BSOD (Blue Screen of Death) is experienced regularly.
- physical disk continues to exhibit excessive activity even when you don’t use it and there is no program or download running at that moment, this could be the right time to check your system for malware.
- running out of hard disk space; there are a number of malicious software which use various methods to fill up all the available space in the hard drive and cause it to crash.
- high network activity is being observed even there is no current connection in the Internet.
- new homepage, new toolbars or unwanted websites being accessed without going there manually using your browsers.
- programs automatically open and close without user intervention and unusual messages seen in the during or after the booting process
- system suddenly shuts down for no reason
- security solution is disabled - your antivirus update is disabled or the antivirus software itself does not work
- strange messages sent from your blogs or emails to your peers via applications in your system that you do not have any control of.

2.2.1.1. Virus

A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether.

2.2.1.2. Worms

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.

2.2.1.3. Trojans

A Trojan horse is another type of malware which functioned the same way as it was named: history foretells that the Greeks gave a huge wooden horse to their foes, the Trojans; after the horse was within the walls of their city, Greek soldiers came out of the hollow horse belly and they were able to capture Troy.

It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create back doors to give malicious users access to the system (a back door is an undocumented way of accessing a system, bypassing the normal authentication mechanisms).

Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the Internet.

2.2.1.4. Bots

"Bot" is derived from the word "robot" and is an automated process that interacts with other network services. Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information (such as web crawlers), or interact automatically with instant messaging (IM), Internet Relay Chat (IRC), or other web interfaces. They may also be used to interact dynamically with websites.

Bots can be used for either good or malicious intent. A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet." With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s). In addition to the worm-like ability to self-propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DoS attacks, relay spam, and open back doors on the infected host.

2.2.2. Phishing

Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and will capture and steal any information the user enters on the page.

The word is a used as a homophone to fishing due to the similarity of using a bait in an attempt to catch a victim. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting victims. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies

2.3. Cybersecurity

The connected electronic information network has become an integral part of our daily lives. All types of organizations, such as medical, financial, and education institutions, use this network to operate effectively. They utilize the network by collecting, processing, storing, and sharing vast amounts of digital information. As more digital information is gathered and shared, the protection of this information is becoming even more vital to our national security and economic stability.

Cybersecurity is the ongoing effort to protect these networked systems and all of the data from unauthorized use or harm. On a personal level, you need to safeguard your identity, your data, and your computing devices. At the corporate level, it is everyone’s responsibility to protect the organization’s reputation, data, and customers. At the state level, national security, and the safety and well-being of the citizens are at stake.

Cyber threats

Your online credentials are valuable. These credentials give the thieves access to your accounts, which in turn will give them access to the money you store in your accounts. A criminal could also take advantage of your relationships. They could access your online accounts and your reputation to trick you into wiring money to your friends or family. This trick which is coined as social engineering allows criminal to send messages stating that your family or friends need you to wire them money so they can get home from abroad after losing their wallets. This technique is also used by these criminals to manipulate people into making them think they are closed friends, but they actually have hidden intentions behind this.

The criminals are very imaginative when they are trying to trick you into giving them money. They do not just steal your money; they could also steal your identity and ruin your life.

There are two types of security threats. Attacks originating from within an organization or from outside of the organization is known as an **internal threat**. An internal user, such as an employee or contract partner, can accidentally or intentionally mishandle confidential data, threaten the operations of internal servers or network infrastructure devices, facilitate outside attacks by connecting infected USB media into the corporate computer system, accidentally invite malware onto the network through malicious email or websites. When the mentioned attacks is done from the outside the facility, this is considered to be an **external threats**. Internal threats also have the potential to cause greater damage than external threats, because internal users have direct access to the building and its infrastructure devices. Employees also have knowledge of the corporate network, its resources, and its confidential data, as well as different levels of user or administrative privileges.

Types of Attackers

Attackers are individuals or groups who attempt to exploit vulnerability for personal or financial gain. Attackers are interested in everything, from credit cards to product designs and anything with value.

Amateurs – These people are sometimes called Script Kiddies. They are usually attackers with little or no skill, often using existing tools or instructions found on the Internet to launch attacks. Some of them are just curious, while others are trying to demonstrate their skills and cause harm. They may be using basic tools, but the results can still be devastating.

Hackers – This group of attackers break into computers or networks to gain access. Depending on the intent of the break-in, these attackers are classified as white, gray, or black hats. The white hat attackers break into networks or computer systems to discover weaknesses so that the security of these systems can be improved. These break-ins are done with prior permission and any results are reported back to the owner. On the other hand, black hat attackers take advantage of any vulnerability for illegal personal, financial or political gain. Gray hat attackers are somewhere between white and black hat attackers. The gray hat attackers may find a vulnerability in a system. Gray hat hackers may report the vulnerability to the owners of the system if that action coincides with their agenda. Some gray hat hackers publish the facts about the vulnerability on the Internet so that other attackers can exploit it.

Organized Hackers – These hackers include organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers. Cyber criminals are usually groups of professional criminals focused on control, power, and wealth. The criminals are highly sophisticated and organized, and they may even provide cybercrime as a service to other criminals. Hacktivists make political statements to create awareness to issues that are important to them. State-sponsored attackers gather intelligence or commit sabotage on behalf of their government. These attackers are usually highly trained and well-funded, and their attacks are focused on specific goals that are beneficial to their government.

The Consequences of a Security Breach

To protect an organization from every possible cyberattack is not feasible, for a few reasons. The expertise necessary to set up and maintain the secure network can be expensive. Attackers will always continue to find new ways to target networks. Eventually, an advanced and targeted cyberattack will succeed. The priority will then be how quickly your security team can respond to the attack to minimize the loss of data, downtime, and revenue.

By now you know that anything posted online can live online forever, even if you were able to erase all the copies in your possession. If your servers were hacked, the confidential personnel information could be made public. A hacker (or hacking group) may vandalize the company website by posting untrue information and ruin the company's reputation that took years to build. The hackers can also take down the company website causing the company to lose revenue. If the website is down for longer periods of time, the company may appear unreliable and possibly lose credibility. If the company website or network has been breached, this could lead to leaked confidential documents, revealed trade secrets, and stolen intellectual property. The loss of all this information may impede company growth and expansion.

The monetary cost of a breach is much higher than just replacing any lost or stolen devices, investing in existing security and strengthening the building's physical security. The company may be responsible for contacting all the affected customers about the breach and may have to be prepared for litigation. With all this turmoil, employees may choose to leave the company. The company may need to focus less on growing and more on repairing its reputation.

Legal Issues in Cybersecurity

Cybersecurity professionals must have the same skills as hackers, especially black hat hackers, in order to protect against attacks. One difference between a hacker and a cybersecurity professional is that the cybersecurity professional must work within legal boundaries.

Personal Legal Issues

You do not even have to be an employee to be subject to cybersecurity laws. In your private life, you may have the opportunity and skills to hack another person's computer or network. There is an old saying, "Just because you can does not mean you should." Keep this in mind. Most hackers leave tracks, whether they know it or not, and these tracks can be followed back to the hacker.

Cybersecurity professionals develop many skills which can be used for good or evil. Those who use their skills within the legal system, to protect infrastructure, networks, and privacy are always in high demand.

Corporate Legal Issues

Most countries have some cybersecurity laws in place. They may have to do with critical infrastructure, networks, and corporate and individual privacy. Businesses are required to abide by these laws.

In some cases, if you break cybersecurity laws while doing your job, it is the company that may be punished and you could lose your job. In other cases, you could be prosecuted, fined, and possibly sentenced.

In general, if you are confused about whether an action or behavior might be illegal, assume that it is illegal and do not do it. Your company may have a legal department or someone in the human resources department who can answer your questions before you do something illegal.

International Law and Cybersecurity

The area of cybersecurity law is much newer than cybersecurity itself. As mentioned before, most countries have some laws in place, and there will be more laws to come.

International cybersecurity law is still quite new. The International Multilateral Partnership Against Cyber Threats (IMPACT) is the first, international public-private partnership that is focused on cyber threats. IMPACT is a global partnership of world governments, industries, and academia dedicated to improving global capabilities when dealing with cyber threats.

What is Cyberwarfare?

Cyberspace has become another important dimension of warfare, where nations can carry out conflicts without the clashes of traditional troops and machines. This allows countries with minimal military presence to be as strong as other nations in cyberspace. Cyberwarfare is an Internet-based conflict that involves the penetration of computer systems and networks of other nations. These attackers have the resources and expertise to launch massive Internet-based attacks against other nations to cause damage or disrupt services, such as shutting down a power grid.

An example of a state-sponsored attack involved the Stuxnet malware that was designed to damage Iran’s nuclear enrichment plant. Stuxnet malware did not hijack targeted computers to steal information. It was designed to damage physical equipment that was controlled by computers, and used modular coding that was programmed to perform a specific task within the malware. It used stolen digital certificates so the attack appeared legitimate to the system.

The main purpose of cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

A nation can continuously invade other nation’s infrastructure, steal defense secrets, and gather information about technology to narrow the gaps in its industries and military. Besides industrial and militaristic espionage, cyberwar can sabotage the infrastructure of other nations and cost lives in the targeted nations. For example, an attack can cause the following:

- disrupt the power grid of a major city.
- traffic would be disrupted
- the exchange of goods and services is halted
- patients cannot get the care needed in emergency situations.
- access to the Internet may also be disrupted.

Furthermore, compromised sensitive data can give the attackers the ability to blackmail personnel within the government. The information may allow an attacker to pretend to be an authorized user to access sensitive information or equipment.

If the government cannot defend against the cyberattacks, the citizens may lose confidence in the government’s ability to protect them. Cyberwarfare can destabilize a nation, disrupt commerce, and affect the citizens’ faith in their government without ever physically invading the targeted nation.

Confidentiality, Integrity, and Availability

Confidentiality, integrity and availability, known as the CIA triad is a guideline for information security for an organization. Confidentiality ensures the privacy of data by restricting access through authentication encryption. Integrity assures that the information is accurate and trustworthy. Availability ensures that the information is accessible to authorized people.

Confidentiality

Another term for confidentiality would be privacy. Company policies should restrict access to the information to authorized personnel and ensure that only those authorized individuals view this data. The data may be compartmentalized according to the security or sensitivity level of the information. For example, a Java program developer should not have to access to the personal information of all employees. Furthermore, employees should receive training to understand the best practices in safeguarding sensitive information to protect themselves and the company from attacks. Methods to ensure confidentiality include data encryption, username ID and password, two factor authentication, and minimizing exposure of sensitive information.

Integrity

Integrity is accuracy, consistency, and trustworthiness of the data during its entire life cycle. Data must be unaltered during transit and is not changed by unauthorized entities. File permissions and user access control can prevent unauthorized access. Version control can be used to prevent accidental changes by authorized users. Backups must be available to restore any corrupted data, and checksum hashing can be used to verify integrity of the data during transfer.

A checksum is used to verify the integrity of files, or strings of characters, after they have been transferred from one device to another across your local network or the Internet. Checksums are calculated with hash functions. Some of the common checksums are MD5, SHA-1, SHA-256, and SHA-512. A hash function uses a mathematical algorithm to transform the data into fixed-length value that represents the data. The hashed value is simply there for comparison. From the hashed value, the original data cannot be retrieved directly. For example, if you forgot your password, your password cannot be recovered from the hashed value. The password must be reset.

Availability

Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It’s also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important. Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues do occur. Fast and adaptive disaster recovery is essential for the worst case scenarios; that capacity is reliant on the existence of a comprehensive disaster recovery plan (DRP). Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to malicious actions such as denial-of-service (DoS) attacks and network intrusions.

2.4. Fighting Against Security Threats

Best Practices for Combating Malware Threats

One should always secure their system from malware attacks. The following steps are recommendations for cybersecurity.

2.4.1. Best Practices for Combating Malware Threats

2.4.1.1. Ensure that your operating system is up to date

This means that you must regularly apply the most recent patches and fixes that is recommended by the OS vendor

2.4.1.2. Install an anti-virus software in your PC's

Also, assure that they are always updated. This can prevent threats like viruses, Trojan horses and malwares from causing damage into your system. The installed software should be email to scan e-mail and files as they are downloaded from the Internet or transferred from external media.

2.4.1.3. Firewall should always be enabled

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks.

2.4.1.4. Assure that the file to be downloaded is safe

Emails usually have attached files which may tend to be unsafe as it may contain viruses and Trojan horses. Assure that your mailing site has anti-virus extensions enabled. In addition, download attachments only from known trusted senders (and at least verify from the sender if he has really sent an email or not).

2.4.1.5. Be cautious accepting or agreeing to prompts

When prompted to install any program or add-on, make sure to read and understand the agreement before clicking on the Ok button. If you do not understand the agreement or feel it is not necessary to install the program, cancel or close the window. Additionally, when installing any program, watch for any check box that asks if it's ok to install a third-party program, toolbar, etc. These are never required and often cause more issues than good. Leave these boxes unchecked.

2.4.2. Points to Ponder to Secure your Own Data

Your personal data can be accessed anywhere. It is up to you how you secure this information from the cyber attackers. No one is safe from these threats, so it is up to you to secure your data and perform appropriate measures to assure safety and security. Remember that the information may be used against you in any way an attacker can, so precautions must be put into consideration.

2.4.2.1. Use browsers in a private manner

especially when surfing in an internet cafe or using others laptops/desktops. Other browsers term this as InPrivate browsing or incognito mode. This mode allows the system not to store any information entered by the user while using the browser. All of the input values will totally be erased once the user closes the browser. However, keep in mind that browser needs to be closed after using it; its feature will be meaningless if the device is left opened while you are still logged in.

2.4.2.2. You should take care when choosing a username or alias for your online identity

The username should not include any personal information. It should be something appropriate and respectful. This username should not lead strangers to think you are an easy target for cybercrimes or unwanted attention.

2.4.2.3. Choose your passwords wisely

As much as possible, choose a password with a combination of uppercase, lowercase, numeric, and special characters. Never use passwords that will include any personal information like your birthday or full name. In addition, never store them in a way that is accessible by anyone.

2.4.2.4. Be careful when sharing documents, pictures, and other online resources via blogs or emails

Once files are downloaded from a public computer shop, make sure that the files are removed from the system before leaving your terminal.

2.4.2.5. Be aware of shoulder surfing

This is an act of looking "past your shoulder" anything that you are typing from the keyboard or on your cellular phones and tablets without you noticing.

2.4.2.6. Verify data is encrypted

When sending confidential information over the Internet, such as usernames, passwords, or credit card numbers, only send it securely. To verify this, look for a small lock in the bottom right corner of your browser window or next to the address bar. If visible, this lock should also be in the locked position and not unlocked. We also suggest making sure the URL begins with https. While the lock is in the locked position, data is encrypted, which helps anyone from understanding the data if it's intercepted. When no lock is visible or in the unlocked position, all information is plaintext and could be read if intercepted. If a web page is not secure, such as an online forum, use a password you wouldn't use with protected sites, such as your online banking website.

2.4.2.7. Be aware of social engineering

This is a psychological manipulation of people into tricking other people until the victim divulge into sharing confidential information.

2.4.2.8. Use two-factor authentication if it is available

Two-factor authentication adds additional protection by requiring an additional step in verifying a login. Typically with two-factor authentication, after verifying your password, if the service does not recognize your computer, it sends your phone a text message with a verification code. If someone had your password but did not have your phone, even with a valid password, they cannot access your account.

2.4.2.9. When connecting via Wi-Fi, log on to a secure network using WEP or WPA

this may prevent nearby users from intercepting and reading information that has been sent to and from your PC.

2.5. Netiquette and Internet Chat Rooms

Netiquette, a colloquial term for network etiquette or Internet etiquette, is a set of social conventions that facilitate interaction over networks.

Like the network itself, these developing norms remain in a state of flux and vary from community to community.The points most strongly emphasized about netiquette often include:

- using simple electronic signatures; this can be done in the settings of the mailing site.
- avoiding multiposting, cross-posting, off-topic posting, hijacking a discussion thread, and other techniques used to minimize the effort required to read a post or a thread.
- use of unabbreviated English while users of instant messaging protocols like SMS occasionally encourage just the opposite, bolstering use of SMS language. However, many online communities frown upon this practice.
- avoid flamewars and spam
- avoid typing in all caps or grossly enlarging script for

emphasis, which is considered to be the equivalent of shouting or yelling.
- Other commonly shared points, such as remembering that one's posts are (or can easily be made) public, are generally intuitively understood by publishers of Web pages and posters to Usenet, although this rule is somewhat flexible depending on the environment. On more private protocols, however, such as e-mail and SMS, some users take the privacy of their posts for granted. One-on-one communications, such as private messages on chat forums and direct SMSs, may be considered more private than other such protocols, but infamous breaches surround even these relatively private media.
- Beyond matters of basic courtesy and privacy, e-mail syntax (defined by RFC 2822) allows for different types of recipients. The primary recipient, defined by the To: line, can reasonably be expected to respond, but recipients of carbon copies cannot be, although they still might. Likewise, misuse of the CC: functions in lieu of traditional mailing lists can result in serious technical issues.

Core Rules of Etiquette

Rule 1: Remember the Human
Rule 2: Adhere to the same standards of behavior online that you follow in real life
Rule 3: Know where you are in cyberspace
Rule 4: Respect other people's time and bandwidth
Rule 5: Make yourself look good online
Rule 6: Share expert knowledge
Rule 7: Help keep flame wars under control
Rule 8: Respect other people's privacy
Rule 9: Don't abuse your power
Rule 10: Be forgiving of other people's mistakes

2.5.1. Email

Electronic mail (e-mail) is a common way of communicating formally with people as you are able to put in your message to whom the message is for (it may be an individual or a group of people), a summary of the message in the Subject field, and some critical information of the sender. When composing an email, you usually fill up the following components:

- To: field: the main recipient of the message; it may contain more than one email addresses
- CC: field: this means carbon copy. This may include email addresses that you wish to have the copy of the mail that you are going to send but are not your direct recipients.
- BCC: field: this means blind carbon copy. This is the same with CC field except that this hides the details of this recipient from the others who will receive this email. This means that the recipients from the To: and CC: fields will not know that the recipient from the BCC: has received the same email.
- Subject: This portion should contain a brief detail of what the message is all about and is considered the title of the email.
- Body: This contains the message of the sender.
- Signature: This is seen at the bottom portion of the email and contains information about the sender - Job Title, Work Address, Contact Number, and many others, to name a few.

2.5.2. Group Chat

This is the quickest way of sending a message to the recipient and are usually embedded in most blog sites. It also shows the status of the receiver which will give you a hint if he is available to read the message or not. The receiver may reply immediately to the message as though he/she is conversing with the other in a telephone.

2.5.3. Usenet

Usenet is a bulletin-type of service containing newsgroups where the users can post messages and these posted messages are distributed via Usenet servers. The messages posted will last only for a limited amount of time known as retention time. Usenet users currently logged in may be able to see and reply to any of the posts given the same channel. Some Usenet providers also allow users to upload/download files from the site.

3. Contextualized Online Search and Research Skills

When your teacher asks you to do your homework and you cannot find the answers from your textbooks, you resort to doing your research. This activity may involve either, if not all, of the following: looking for the needed articles from your school library, from references bought from school supply stores, or surfing the Internet.

Research is an integral part of students' life in creating presentations, solving scientific problems, and searching for the definition of an unknown term, but there's more to these activities than what the students usually do. For professionals and academicians, a research assists them in developing new theories, proposing a new solution to an existing problem, or analyzing historical information to determine the origins of a certain person, object or an event.