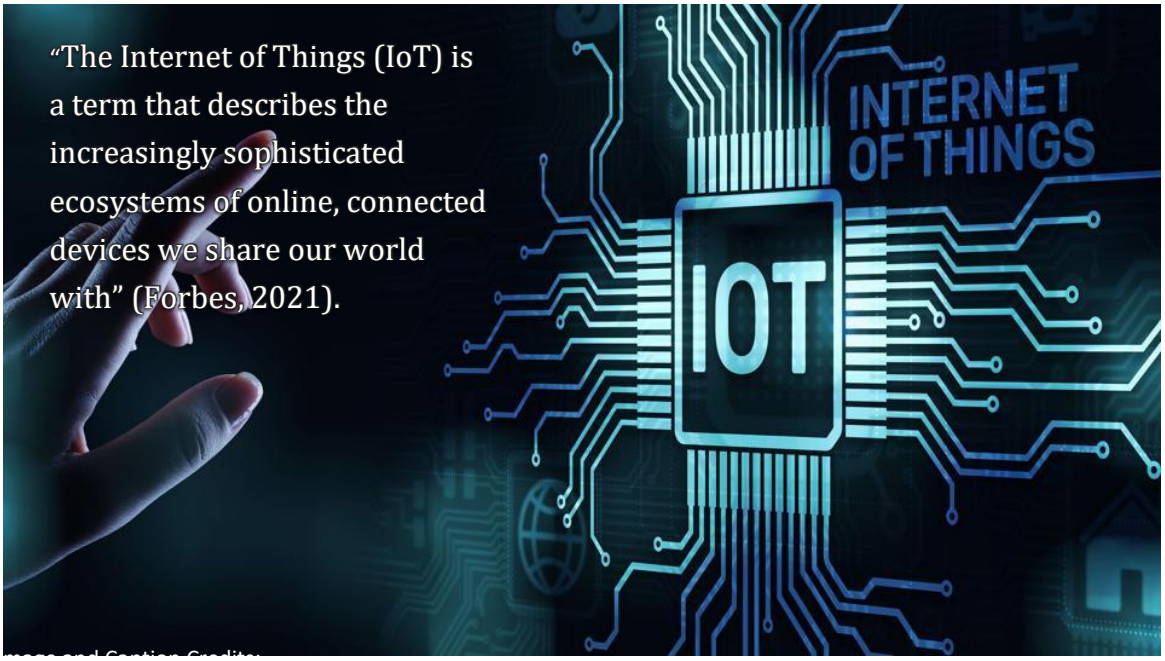
Lecture No. 6

Information, Media, and Cyber Literacy

Becoming a responsible and productive cybercitizen in the 21st century



https://www.forbes.com/sites/bernardmarr/2021/12/13/the-5-biggest-internet-of-things-iot-trends-in-2022/?sh=7f755d0c5aba

Before the COVID-19 Pandemic, we were comfortable utilizing traditional face-to-face classroom teaching and learning interaction. Technological digital devices and online resources were just for reinforcement and enrichment of learning.

Schools were shut down at the height of the pandemic crisis, and we were forced to conduct 100% home-based distance learning for almost two years. During this time, we relied entirely on ourselves to perform independent studies and achieve the learning outcomes set by the curriculum.

Somehow, these radical experiences taught us a lesson to advance to higher technology utilization in education and enjoy the benefits, as well as be cautious of the risks of online resources.

Let's continue from the Conclusions in Lecture 5

Opportunities for future literacy teaching and learning can be found in the incorporation of new literacies and the teaching of multiliteracies. With multiliteracies, educators can ensure that all learners have the same opportunities to study. Students acquire the ability to work together by discussing and debating ideas in virtual or on-campus classrooms that facilitate several learning styles. As a result, the new literacy integration in the teacher education curriculum should help students gain confidence and expertise as they study together in cooperative settings.

Every aspect of our endeavor, whether at home, in the classroom, or elsewhere, involves technology. Yet, there are times when we may not realize that we are misusing or abusing it or when others may exploit us for their evil purposes using digital technologies. As a result, we risk being held accountable for, or even the target of, irresponsible technical processing and application. Whether for professional or personal reasons, we must improve our digital or cyber literacy in this context.

With all these issues, let's be guided by the following objectives in this lecture.

1. Define digital and cyber information literacy in the context of education;
2. Discuss cybersecurity and cyber citizenship and suggest cyber-management and precautionary measures in the use of internet-based tools; and,
3. Integrate digital or cyber literacy into the curriculum.

Let's go ahead.

1. Digital and Cyber Literacy

Digital Literacy Defined. The internet and other forms of contemporary technology have fundamentally altered how people interact with one another and run their businesses, which has led to an educational revolution. The capacity to utilize digital technology successfully to locate information, analyze sources, produce content, and interact with others is called **digital literacy** (Maryville University at https://online.maryville.edu/blog/digital-literacy-a-comprehensive-guide-to-modern-education-technology). It is a set of skills utilized to traverse the new technology paradigm in which society functions. A high level of digital literacy is tremendously beneficial for an efficient learner in an online setting.

Image Credits: https://www.philstar.com/news-commentary/2021/08/21/2121623/information-literacy-learning-spot-what-and-what-isnt-online

The digital literacy spectrum comprises a wide variety of skills and tools. A solid foundation for strong technical skills and experience includes utilizing computers and mobile devices, accessing information online, and engaging with people online through social media. Each of these abilities is a crucial building block.

Cyber Citizenship in Research. Education and research are intertwined in making the teaching and learning experiences knowledge-based, practical, and progressive. With its online resources, the internet has become the leading portal to access information and content for knowledge development, evaluation, and creation.

Image Credits: https://www.philstar.com/headlines/2021/02/17/2078469/groups-surveys-air-concern-looming-learning-crisis-philippines

In this aspect of consideration, properly observing cyber literacy can be termed cyber citizenship. De Leon (2020, p.142) defines cyber citizenship as "being responsible when using the internet" for whatever purpose, especially in accessing and consuming information. What people do online when no one is watching them in private says a lot about their character and morality. Our digital world comes with a lot of power, which also comes with many duties and repercussions. So, we can investigate and access all of the information available online; but we should practice good cyber citizenship.

Cybercitizenship and Cybersecurity. Cybercitizenship is not only concerned with extracting information and doing research online. It also involves how we share information online, commonly through social media.

Cybercitizenship goes with cybersecurity. Cybersecurity refers to the process of preventing and responding to malicious cyber activity. The goals of most cyber assaults are to gain access to, modify, or delete sensitive information; steal money from users; or disrupt corporate operations.

2. Cybersecurity and Cyber Management

There are more connected gadgets than humans, and sophisticated cyber criminals always find new ways to bypass security safeguards. The following are the suggested ways to protect yourself from cyber threats:

Image courtesy of: https://imgbin.com

"Think before you click." – This is a trendy line to caution internet users; specifically those using their social media accounts, reminding them that we need to think critically about the possible consequences of publishing content, images, comments, and other messages. Also, personal information and whereabouts posted on the internet could serve as tips to cybercriminals.

"Fishing by Phishing" – Some suspicious emails that you receive could be forms of phishing. Proofpoint.com defines "Phishing" as "when attackers send malicious emails to trick people into falling for a scam. Typically, the intent is to get users to reveal financial information, system credentials, or other sensitive data" (https://www.proofpoint.com/us/threat-reference/phishing#:~:text=Phishing%20is%20when%20attackers%20send,credentials%20or%20other%20sensitive%20data).

"Algorithms in the Rhythm" – Computer processes use algorithms in data operations and sequences. They are like problem-solving matters that establish formulas and are saved in the computer's history. When surfing the internet, using your online account sends the cloud algorithms that tag your account based on your online behavior. Your history of visiting websites, links, and other internet content is remembered in this sense, including your user IDs and passwords. If someone else uses your device, your private information and access data may be doomed to be obtained. It is often helpful to delete internet history regularly and log out accounts from devices that other people also use.

"Better Safe than Sorry" – Internet-based activities that are improperly handled could cost you a lot. These include suspicious emails, pop-ups, viruses, malware, malicious content, and other dubious features on the internet. Set up credible anti-virus software on your computer, and never open sites and emails you are unsure of.

3. Integrating Digital/Cyber Literacy into the Curriculum

(Adapted from De Leon, 2020, p.154)

The following are suggested activities to integrate digital literacy, higher-order thinking, and constructing meaning in the post-pandemic classroom.

a. Use an interactive whiteboard to design and deliver lessons.
b. Allow students to maintain blogs, wikis, or web pages related to their learning.
c. Engage in online messaging and teleconsultation with the students.
d. Continue using a Learning Management System (LMS) to reinforce on-campus teaching-learning experiences.
e. Encourage learners to present the synthesis of the lesson using multimedia tools, software, and applications.
f. Reinforce traditional classroom instruction with online synchronous learning modes and virtual conferences (blended or hybrid learning).
g. Incorporate netiquette and cyber ethics when using and citing online resources.
h. Nurture collaborative works using online and offline digital procedures.

i. Urge students to document learning experiences using audio-video capturing devices with guidance on data privacy and informed consent standards.

j. Require an E-Portfolio that would compile their outputs, projects, and other evidence of learning.

Conclusion

Digital literacy, also known as cyber literacy, is an assortment of skills effectively using digital devices for communication, expression, collaboration, and empowerment. On the other hand, cybersecurity refers to the practice of safeguarding systems, networks, and programs against digital assaults.

References:

De Leon, E.B. (2020). Building and Enhancing New Literacies Across the Curriculum. Quezon City: LORIMAR

Department of Education Order No. 42, series of 2017 (Republic of the Philippines): https://www.deped.gov.ph/wp-content/uploads/2017/08/DO_s2017_042-1.pdf

Maryville University: https://online.maryville.edu/blog/digital-literacy-a-comprehensive-guide-to-modern-education-technology/#:~:text=What%20is%20digital%20literacy%3F,paradigm%20in%20which%20society%20operates.