11

SENIOR HIGH SCHOOL

DEPARTMENT OF EDUCATION
SCHOOLS DIVISION OF NEGROS ORIENTAL
REGION VII
Kagawasan Ave., Daro, Dumaguete City, Negros Oriental

EMPOWERMENT TECHNOLOGIES
Quarter 3 - Module 2
Online Safety, Security, Ethics andEtiquette Standards

ALTERNATIVE DELIVERY MODE
ADM

Trends, Networks, and Critical Thinking in the 21st Century
Alternative Delivery Mode
Quarter 3 – Module 2: Online Safety, Security, Ethics, and Etiquette Standards
Second Edition, 2021

Published by the Department of EducationSecretary: Leonor Magtolis - Briones
Undersecretary: Diosdado M. San Antonio

Development Team of the Module

Writer: Jessie V. Alcala

Editor: Reynald M. Manzano

Reviewers: Louelyn M. Lajot, Ruth Marie B. Eltanal, Ericson B. Elnar

Layout Artist:

Management Team: Senen Priscillo P. Paulin, CESO V
Marcelo K. Palispis, EdD
Joelyza M. Arcilla, EdD
Nilita L. Ragay, EdD
Antonio B. Baguio Jr., EdD
Rosela R. Abiera
Maricel S. Rasid
Elmar L. Cabrera

Printed in the Philippines by ____________________________

Department of Education –Region VII Schools Division of Negros Oriental

Office Address:	Kagawasan, Ave., Daro, Dumaguete City, Negros Oriental
Tele #:	(035) 225 2376 / 541 1117
E-mail Address:	negros.oriental@deped.gov.ph

Introductory Message

This Self-Learning Module (SLM) is prepared so that you, our dear learners, can continue your studies and learn while at home. Activities, questions, directions, exercises, and discussions are carefully stated for you to understand each lesson.

Each SLM is composed of different parts. Each part shall guide you step-by-step as you discover and understand the lesson prepared for you.

Pre-tests are provided to measure your prior knowledge on lessons in each SLM. This will tell you if you need to proceed on completing this module or if you need to ask your facilitator or your teacher's assistance for better understanding of the lesson. At the end of each module, you need to answer the post-test to self-check your learning. Answer keys are provided for each activity and test. We trust that you will be honest in using these.

In addition to the material in the main text, Notes to the Teacher are also provided to our facilitators and parents for strategies and reminders on how they can best help you on your home-based learning.

Please use this module with care. Do not put unnecessary marks on any part of this SLM. Use a separate sheet of paper in answering the exercises and tests. And read the instructions carefully before performing each task.

If you have any questions in using this SLM or any difficulty in answering the tasks in this module, do not hesitate to consult your teacher or facilitator.

Thank you.

What I Need to Know

With you in mind, this module was created and written. Its purpose is to assist you in understanding the context of Empowerment Technologies. It includes a variety of activities that can assist you in succeeding in contexts that involve the usage of a computer and the Internet as a Senior High School student.

Students will learn about Online Safety, Security, Ethics, and Etiquette Standards in this session, which will help them grasp the world of ICT.

Happy learning!

MOST ESSENTIAL LEARNING COMPETENCIES:

- Apply online safety, security, ethics, and etiquette standards and practice in the use of ICTs as it would relate to their specific professional tracks.
  (CS_ICT11/12-ICTPT-Ia-b- 2)

After going through this module, you are expected to:

K: determine the dangers of the internet
S: consider one's safety when sharing information on the internet
A: Be responsible in the use of social networking sites

What I Know

Direction: Write **True** if you agree or **False** if you do not agree with the statements below.

________ 1. Add someone in Facebook even if you don't know the person to have many friends.
________ 2. Read the terms and conditions before accepting it.
________ 3. You can share your password with your sister.
________ 4. Do not talk to strangers.
________ 5. Only download music or video from a trusted website.
________ 6. Letting people know your birthday in Facebook is a must if you want to get many gifts.
________ 7. You can use a pirated software for personal use only.

________8. Avoid replying to negative comments with more negative comments.

________9. It is okay to share photos or videos of your friend in your social media account.

________10. You should not add a password to your Wifi at home.

________11. Be mindful of what you share and what site you share it to.

________12. Install many antiviruses to ensure protection to your computer.

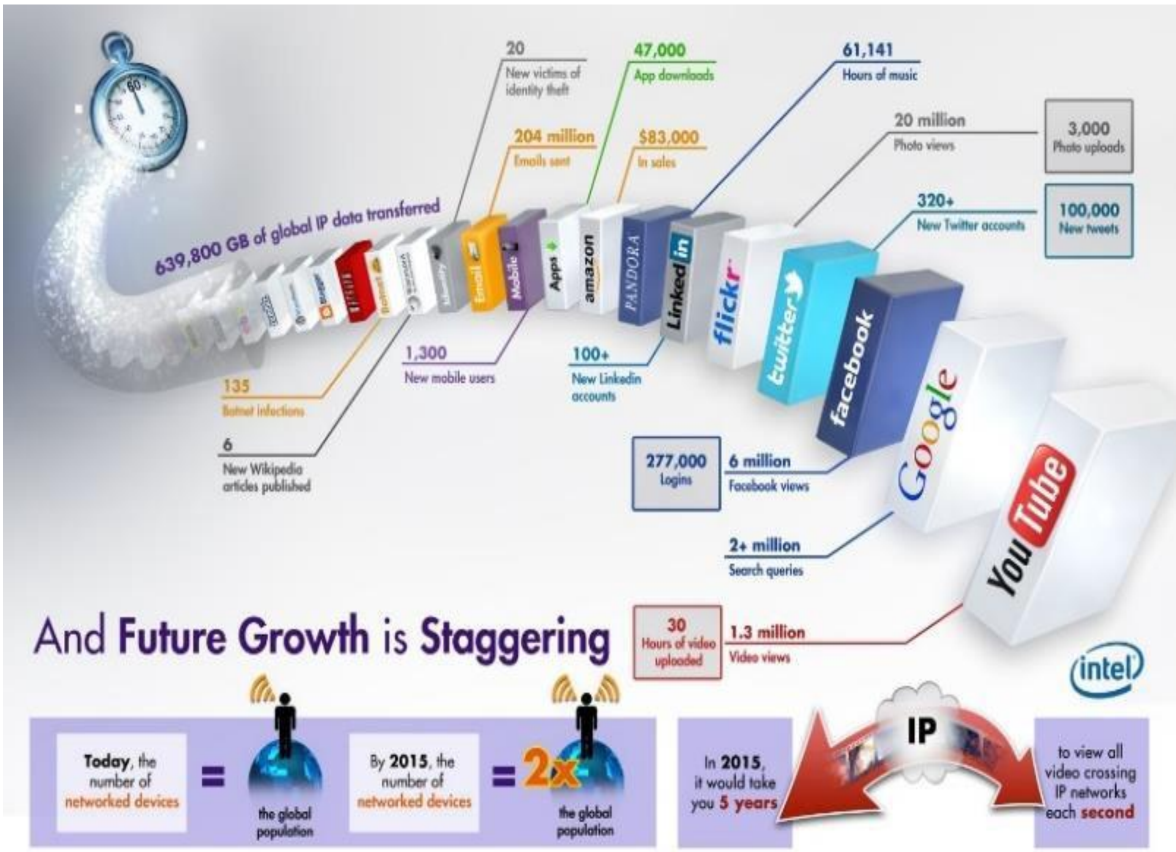
________13. There is a danger for posting future vacation.

________14. Avoid logging in to free WIFI.

________15. It is okay to open any attachments or clicking ads if you have anantivirus in your computer.

What's New

What happens in a minute on the Internet?



(CapacityCreative, 2014)

The picture above shows the speed at which the Internet is changing the world. The sites we visit are so overwhelmingly popular to both adults and children. The online world is increasingly integrated into our daily lives.

The Internet, like the physical world, maybe safe or unsafe dependingon our habits. Sometimes, we do not pay much attention about the information that we share online.

Are you safe and secured online? Using the table below, identify which among the types of information have you shared or not shared?

Type of Information	Shared	Not Shared
First name		
Last name		
Middle name		
Current and previous schools		
Cellphone Number		
Name of your parents		
Name of your siblings		
Address		
Home phone number		
Birthday		

Most likely, you responded with shared in the first two items. If that's the case, then try typing your first and last names into a search engine like Google. Have you received any connections to your profile page? Is it possible to be found by search engines?

What is It

Online Safety, Security, and Etiquette Standards

The Internet is defined as the information superhighway. This means that everyone with access to this highway has the ability to place and retrieve information. The larger the risk, the more information you share online. Identity theft, phishing, malware infestations, and other threats are all possible. As a result, Facebook is constantly improving its security features.

Tips to Stay Safe Online

Here are some tips to help you stay safe when using the Internet.

1. Be mindful of what you share and what site you share it to.
2. Do not just accept terms and conditions; read it.
3. Check out the privacy policy page of a website.
4. Know the security features of the social networking site you use.
5. Passwords should not be shared with anyone. Your password should be treated like a toothbrush. Allow no one to use it, and replace it every six months.
6. Logging into public networks/Wi-Fi is a bad idea. Hackers' ability to position themselves between you and the connection point is one of the most serious dangers to free WiFi. As a result, instead of speaking directly with the hotspot, you send your data to the hacker. Any information you provide or gain access to on these networks is gone in a blink of an eye.
7. Do not talk to strangers whether online or face-to-face.
8. Never post anything about future vacation. You are inviting the burglarto rob your house at that date.
9. Add friends you know in real life.
10. Avoid visiting untrusted websites.
11. On your computer, install and update antivirus software. To avoid conflicts, use only one antivirus software.
12. If you have a Wi-Fi at home, make it a private network by adding a password.
13. Downloading anything from untrusted websites is a bad idea. Malware can infect your computer if you visit certain websites.
14. Buy the software; do not use pirated ones.
15. Do not reply or click links from suspicious emails.

Even if your profile is already set to private, hackers can find a backdoor and steal your information online, thus it is your responsibility to secure it. A hacker may steal information in order to harm people through identity theft, damage or shut down systems, and, in certain cases, keep those systems hostage in exchange for a ransom payment.

Internet Threats

While the internet is an excellent source of communication and information, there are a lot of dangerous risks to be aware of. When utilizing the Internet, here are some of the hazards you should be aware of.

1. Spam

Most of our email accounts come with a ‘Spam’ or ‘Junk’folder. Spam emails are a huge issue, with more than 50% of emails being syphoned into these folders. Asidefrom being an annoyance, spam emails are not a direct threat, but many can contain malware.

2. Adware

When a person surfs the internet, adware is a sort of virus that displays unwanted advertisements. A valid technique of generating advertising money that help fund development is frequently included in many shareware or freeware downloads. Some websites, on the other hand, are tainted with dangerous adware that is downloaded to your computer automatically.

3. Trojan

Trojans leave your computer vulnerable to hackers, allowing them to steal any data on your computer. Trojans frequently disguise themselves as harmless computer programs in order for hackers to gain access to your computer without being detected by you.

4. Virus

A virus is one of the most talked about internet threats. Because viruses are designed to propagate at an alarming rate, they usually attach themselves discreetly to downloads. Antivirus software is often attached to files for download, shares virus-infected email attachments, or loaded onto computers via CDs, DVDs, and USB sticks.

5. Worms

Malicious email attachments or USB sticks are the most common ways for worms to get onto a computer. When a worm infects your computer, it will most likely send itself to every email account on your machine. Your email will appear innocent to the recipient until they read it and find themselves infected by the same worm.

6. Phishing

Phishing is a type of fraudulent behavior in its most basic form. Official-looking emails impersonating a well-known source, such as a bank, are frequently sent. It is the purpose of these emails to acquire people's passwords and credit card information.

7. Spyware

Spyware is another type of malware. Known as spyware, it is an all-encompassing internet ailment that is commonly associated with downloading file pop-ups. Spyware can monitor your keystrokes, read, and destroy your files, reformat your hard drive, and access your apps once it is installed on your computer. Without your knowledge, the individual in charge of the spyware has access to your personal information.

8. Keyloggers

Keyloggers, which are similar to spyware, record a user's keyboard operations. The majority of keyloggers will hunt for easily identifiable key entries, such as bank card numbers and passwords. Identity and intellectual property theft are frequently tied to keylogging.

9. Pharming

Pharming is a more sophisticated form of phishing that takes advantage of the DNS system. Pharmers frequently construct web pages that look like those of a reputable company, such as an online banking log-in page. Users will then submit their credentials, assuming they are logging in to their regular service, and the pharmer will steal their credentials.

10. Rogue Security Software

This is a form of malicious software and internet fraud that misleads users into believing there is a virus on their computer and aims to convince themto pay for a fake malware removal tool that actually installs malware on their computer.

Netiquette

Netiquette is a short for "Internet etiquette," and it is a code of appropriate online behavior that is similar to politeness in society. Email, social media, online chat, web forums, website comments, multiplayer gaming, and other forms of online communication are all examples of this.

While there is no official list of netiquette rules or guidelines, the general idea is to respect others online. Below are tenexamples of rules to follow for good netiquette:

1. Avoid posting inflammatory or offensive comments online (aka flaming).
2. Respect others' privacy by not sharing personal information, photos, or videos that another person may not want published online.
3. Never spam others by sending large amounts of unsolicited email.
4. Show good sportsmanship when playing online games, whether you win or lose.
5. Don't troll people in web forums or website comments by repeatedly nagging or annoying them.
6. Stick to the topic when posting in online forums or when commenting on photos or videos, such as YouTube or Facebook comments.
7. Don't swear or use offensive language.
8. Avoid replying to negative comments with more negative comments. Instead, break the cycle with a positive post.
9. If someone asks a question and you know the answer, offer to help.
10. Thank others who help you online.

Because you rarely see or hear the people with whom you communicate online, the Internet provides a sense of anonymity. That isn't to say that you can't have bad manners or make provocative statements. Some people believe they can hide behind their keyboard or smartphone when it comes to posting online, but the truth is that they are the ones who are actually publishing the content. Remember that if you make inappropriate comments online and the veil of anonymity is gone, you will be held accountable for your actions.

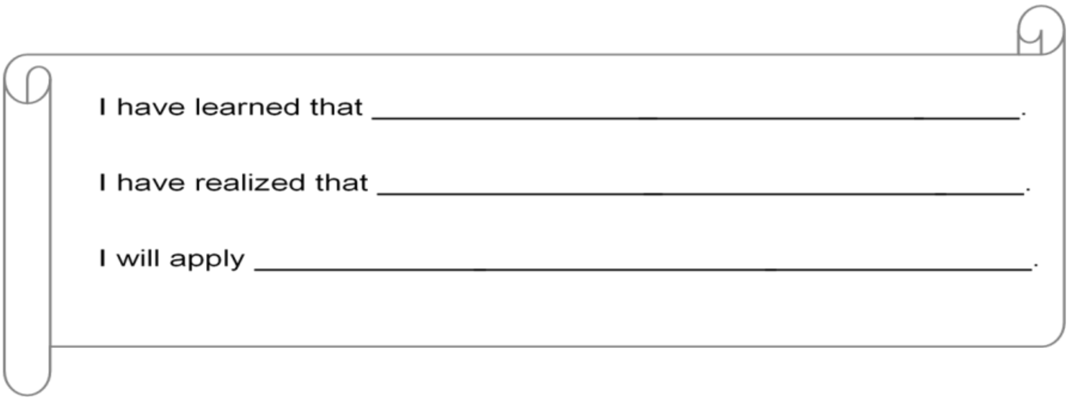
In summary, good netiquette benefits both you and others on the Internet. Posting a positive comment rather than a negative one just might make someone's day.

What's More

Direction: Visit a social networking site and look for the site's privacy policy. Write a summary on how the website handles your private and public information. Write your answer on your notebook.

What I Have Learned

Instruction: Make a journal to manifest your understanding about the topic. You can start by following the format below. Write it on your notebook.



I have learned that ______________________________________.

I have realized that ______________________________________.

I will apply ____.

What I Can Do

Direction: Create a poster promoting "Think before you click". Post it in your social media site as an awareness program for your friends. (*If internet connection isnot available, do your poster on a bond paper and submit it to your teacher).*

Rubric

CATEGORY	**4**	**3**	**2**	**1**
Required Elements	The poster includes all required elements as well as additional information.	All required elements are included on the poster.	All but 1 of the required elements are included on the poster.	Several required elements were missing.
Labels	All items of importance on the poster are clearly labeled with labels that can be read from at least 3 feet away.	Almost all items of importance on the poster are clearly labeled with labels that can be read from at least 3 feet away.	Many items of importance on the poster are clearly labeled with labels that can be read from at least 3 feet away.	Labels are too small to view OR no important items were labeled.
Graphics - Relevance	All graphics are related to the topic and make it easier to understand. All borrowed graphics have a source citation.	All graphics are related to the topic and most make it easier to understand. Some borrowed graphics have a source citation.	All graphics relate to the topic. One or two borrowed graphics have a source citation.	Graphics do not relate to the topic OR several borrowed graphics do not have a source citation.
Layout and design	The poster is exceptionally attractive in terms of design, layout, and neatness.	The poster is attractive in terms of design, layout, and neatness.	The poster is acceptably attractive though it may be a bit messy.	The poster is distractingly messy or very poorly designed. It is not attractive.
Organization	There are no grammatical/mechanical mistakes on the poster.	There are 1-2 grammatical/mechanical mistakes on the poster.	There are 3-4 grammatical/mechanical mistakes on the poster.	There are more than 4 grammatical/ mechanical

				mistakes on the poster

Assessment

I. Match Column A with Column B. Read each item carefully and use your notebook to write your answers.

Answers	A	B
________1.	It displays unwanted ads when a user is surfing the internet.	a. Spyware b. Rogue security software c. Adware d. Worm e. Keylogging f. Netiquette g. Virus h. Trojans i. Spam j. Phishing k. Pharmers l. Internet
________2.	This is a form of malicious software and internet fraud that misleads users into believing there is a virus on their computer and convince them to pay for a fake malware removal tool.	
________3.	They present themselves as harmless computer programs so that hackers can penetrate your computer without being detected.	
________4.	It can monitor your keystrokes, read and delete your files, reformat your hard drive, and access your applications.	
________5.	These are unwanted emails.	
________6.	They usually make their way on to a computer via a malicious email attachment or USB stick.	
________7.	They are often attached to files for download, shared via CDs, DVDs, and USB sticks, or loaded on to computers by opening infected email attachments.	
________8.	These are official-looking emails that are sent impersonating a well-known provider, such as a bank.	

________9.	This is often linked to identity and intellectual property theft.	
________10.	A code of good behavior on the Internet.	
________11.	This is defined as an information superhighway.	
________12.	They create web pages mimicking that of a trustworthy business, such as an online banking log-in page.	
________13.	This records a user’s keyboard input.	
________14.	This is not a direct threat but many can contain malware.	
________15.	It leaves your computer completely unprotected.	

Additional Activities

Direction: Research about cybercrime news. Using any video-recording device, report it as if you were a newscaster. Save your file and send it to your teacher.

Answer Key

What I Know

1. False
2. True
3. False
4. True
5. True
6. False
7. False
8. True
9. False
10. False
11. True
12. False
13. True
14. True
15. False

Assessment

1. C
2. B
3. H
4. A
5. I
6. D
7. G
8. J
9. E
10. F
11. L
12. K
13. E
14. I
15. H

References

Rex Book Store.(2016).Empowerment Technologies.1.17-25

“Netiquette.” Netiquette Definition. Accessed February 17, 2021. https://techterms.com/definition/netiquette.

Luminet. 2016. *https://luminet.co.uk.* December 14. Accessed February 17, 2021. https://luminet.co.uk/top-10-common-internet-threats/.

Oxillo, Mark Jhon. 2017. *https://www.slideshare.net.* November 24. Accessed February 17, 2021. https://www.slideshare.net/markjhonoxillo/empowerment-technologies-online-safety-security-ethics-and-netiquette?qid=73539e55-b525-4d92-89bb-c2881ed0ad97&v=&b=&from_search=10.

Rosencrance, Linda. 2017. *https://searchsecurity.techtarget.com.* August. Accessed February 17,2021. https://searchsecurity.techtarget.com/definition/hacker.

“What Happens in an Internet Minute [Infographic].” Cap City Creative - A Creative Solutions Agency, February 10, 2014. https://www.capcitycreative.ca/happens-internet-minute-infographic/.

For inquiries or feedback, please write or call:

Department of Education – Schools Division of Negros Oriental
Kagawasan, Avenue, Daro, Dumaguete City, Negros Oriental

Tel #: (035) 225 2376 / 541 1117
Email Address: negros.oriental@deped.gov.ph
Website: lrmds.depednodis.net