



**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 and Etiquette Standards



GOVERNMENT PROPERTY
NOT FOR SALE

Trends, Networks, and Critical Thinking in the 21st Century
Alternative Delivery Mode
Quarter 3 – Module 2: Online Safety, Security, Ethics, and Etiquette Standards
First Edition, 2020

Republic Act 8293, section 176 states that: No copyright shall subsist in any work of the Government of the Philippines. However, prior approval of the government agency or office wherein the work is created shall be necessary for exploitation of such work for profit. Such agency or office may, among other things, impose as a condition the payment of royalties.

Borrowed materials (i.e., songs, stories, poems, pictures, photos, brand names, trademarks, etc.) included in this module are owned by their respective copyright holders. Every effort has been exerted to locate and seek permission to use these materials from their respective copyright owners. The publisher and authors do not represent nor claim ownership over them.

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

Development Team of the Module

Writer:	Jessie V. Alcala	
Editor:	Reynald M. Manzano	
Reviewer:	Louelyn M.Lajot, Ruth Marie B. Eltanal	
Layout Artist:		
Management Team:	Senen Priscillo P. Paulin, CESO V	Rosela R. Abiera
	Fay C. Luarez, TM, Ed.D., Ph.D.	Maricel S. Rasid
	Nilita L. Ragay, Ed.D.	Elmar L. Cabrera
	Antonio B. Baguio, Jr., Ed.D.	

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

EMPOWERMENT TECHNOLOGIES

**Quarter 3 – Module 2:
Online Safety, Security, Ethics, and
Etiquette Standards**



Introductory Message

For the facilitator:

Welcome to the Empowerment Technologies Alternative Delivery Mode (ADM) Module on Online Safety, Security, Ethics, and Etiquette Standards!

This module was collaboratively designed, developed and reviewed by educators both from public and private institutions to assist you, the teacher or facilitator in helping the learners meet the standards set by the K to 12 Curriculum while overcoming their personal, social, and economic constraints in schooling.

This learning resource hopes to engage the learners into guided and independent learning activities at their own pace and time. Furthermore, this also aims to help learners acquire the needed 21st century skills while taking into consideration their needs and circumstances.

In addition to the material in the main text, you will also see this box in the body of the module:



Notes to the Teacher

This contains helpful tips or strategies that will help you in guiding the learners.










As a facilitator, you are expected to orient the learners on how to use this module. You also need to keep track of the learners' progress while allowing them to manage their own learning. Furthermore, you are expected to encourage and assist the learners as they do the tasks included in the module.



For the learner:

Welcome to the Empowerment Technologies Alternative Delivery Mode (ADM)
Module on Online Safety, Security, Ethics, and Etiquette Standards!

This module was designed to provide you with fun and meaningful opportunities for guided and independent learning at your own pace and time. You will be enabled to process the contents of the learning resource while being an active learner.

This module has the following parts and corresponding icons:

 <i>What I Need to Know</i>	This will give you an idea of the skills or competencies you are expected to learn in the module.
 <i>What I Know</i>	This part includes an activity that aims to check what you already know about the lesson to take. If you get all the answers correct (100%), you may decide to skip this module.
 <i>What's In</i>	This is a brief drill or review to help you link the current lesson with the previous one.
 <i>What's New</i>	In this portion, the new lesson will be introduced to you in various ways; a story, a song, a poem, a problem opener, an activity or a situation.
 <i>What is It</i>	This section provides a brief discussion of the lesson. This aims to help you discover and understand new concepts and skills.
 <i>What's More</i>	This comprises activities for independent practice to solidify your understanding and skills of the topic. You may check the answers to the exercises using the Answer Key at the end of the module.
 <i>What I Have Learned</i>	This includes questions or blank sentence/paragraph to be filled in to process what you learned from the lesson.
 <i>What I Can Do</i>	This section provides an activity which will help you transfer your new knowledge or skill into real life situations or concerns.
 <i>Assessment</i>	This is a task which aims to evaluate your level of mastery in achieving the learning competency.

 Additional Activities	In this portion, another activity will be given to you to enrich your knowledge or skill of the lesson learned.
 Answer Key	This contains answers to all activities in the module.

At the end of this module you will also find:

References

This is a list of all sources used in developing this module.

The following are some reminders in using this module:

1. Use the module with care. Do not put unnecessary mark/s on any part of the module. Use a separate sheet of paper in answering the exercises.
2. Don't forget to answer *What I Know* before moving on to the other activities included in the module.
3. Read the instruction carefully before doing each task.
4. Observe honesty and integrity in doing the tasks and checking your answers.
5. Finish the task at hand before proceeding to the next.
6. Return this module to your teacher/facilitator once you are through with it.

If you encounter any difficulty in answering the tasks in this module, do not hesitate to consult your teacher or facilitator. Always bear in mind that you are not alone.

We hope that through this material, you will experience meaningful learning and gain deep understanding of the relevant competencies. You can do it!



What I Need to Know

This module was designed and written with you in mind. It is here to help you master the context of Empowerment Technologies. It contains varied activities that can help you as a Senior High School student to succeed in environments that require the use of computer and the Internet.

The module contains lessons in Online Safety, Security, Ethics, and Etiquette Standards which allows students to understand 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 in 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 antivirus 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 an antivirus in your computer.



What's New

What happens in a minute in the Internet?



<https://www.cancitvcreative.ca/happens-internet-minute-infographic/>

This picture 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 depending on 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		

You probably answered shared in the first two items. If that is the case. Try using a search engine like google then type your first and last name. Did you get links to your profile page? Is there any danger of being found by search engines?



What is It

Online Safety, Security, and Etiquette Standards

The Internet is defined as the information superhighway. This means that anyone has access to this highway, can place information, and can grab that information. The more information you share online, the higher the risk. Risk such as identity theft, phishing, malware infections, and the likes. That is why Facebook continues to improve their 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. Do not share password with anyone. Treat your password like a toothbrush. Don't let anybody use it and get a new one every six months.
6. Avoid logging in to public networks/Wi-Fi. One of the biggest threats with free WiFi is the ability for hackers to position themselves between you and the connection point. So, instead of talking directly with the hotspot, you end up sending your information to the hacker. ... Any information you share or access on these networks is as good as gone.
7. Do not talk to strangers whether online or face-to-face.
8. Never post anything about future vacation. You are inviting the burglar to rob your house at that date.
9. Add friends you know in real life.
10. Avoid visiting untrusted websites.
11. Install and update an antivirus software on your computer. Use only one antivirus software to avoid conflict.
12. If you have a Wi-Fi at home, make it a private network by adding a password.
13. Avoid downloading anything from untrusted websites. Some websites carry malwares that can infect your computer.
14. Buy the software; do not use pirated ones.
15. Do not reply or click links from suspicious emails.

It is your responsibility to secure your information online because there are hackers who can find a backdoor even if your profile is already set to private. A hacker may steal information to hurt people via identity theft, damage or bring down systems and, often, hold those systems hostage to collect ransom.

Internet Threats



Whilst the internet is a fantastic place for communication and information, there are many malicious threats you need to dodge along the way. Here are some of the threats you should be aware of when using the Internet.

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. Aside from being an annoyance, spam emails are not a direct threat, but, many can contain malware.

2. **Adware**

Adware is a type of malware software that displays unwanted ads when a user is surfing the internet. It is often included in many shareware or freeware downloads as a legitimate way of generating advertising revenues that help fund development. However, some websites are infected with malicious adware that are automatically downloaded to your computer.

3. **Trojan**

Trojans leave your computer completely unprotected, which can mean that hackers can steal any data from your system. Trojans often present themselves as harmless computer programs so that hackers can penetrate your computer without being detected.

4. **Virus**

One of the most talked about internet threats is a virus. Viruses usually attach themselves covertly to downloads as they are designed to spread at an alarming rate. Viruses are often attached to files for download, shared via CDs, DVDs, and USB sticks, or loaded on to computers by opening infected email attachments.

5. **Worms**

Worms usually make their way on to a computer via a malicious email attachment or USB stick. Once your computer has been infected by a worm, it will likely send itself to every email address logged in your system. To the receiver, your email will appear harmless, until they open it and are infected by the same worm.

6. **Phishing**

In its simplest terms, phishing is a form of fraudulent activity. More often than not, official-looking emails are sent impersonating a well-known provider, such as a bank. These emails are sent to acquire people's passwords and credit card details.

7. **Spyware**

Another form of malware is spyware. Spyware is an all-encompassing internet nasty and is usually attached to pop-ups of downloadable files. Once installed on your computer, spyware can monitor your keystrokes, read and delete your files, reformat your hard drive, and access your applications. Whoever is controlling the spyware has access to your personal details without you even knowing.

8. **Keyloggers**

Similar to a part of spyware, keyloggers record a user's keyboard actions. Most keyloggers will be looking for distinguishable key entries, such as bank card details and passwords. Keylogging is often linked to identity and intellectual property theft.

9. **Pharming**

Pharming is a more complex version of phishing that exploits the DNS system. Pharmers often create web pages mimicking that of a trustworthy business, such as an online banking log-in page. Users will then enter their details, thinking they are logging in to their usual service, and their details will be stolen by the pharmer.

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 them to pay for a fake malware removal tool that actually installs malware on their computer.

Netiquette

Netiquette is short for "Internet etiquette." Just like etiquette is a code of polite behavior in society, netiquette is a code of good behavior on the Internet. This includes several aspects of the Internet, such as email, social media, online chat, web forums, website comments, multiplayer gaming, and other types of online communication.



<https://www.eu-in-the-media.eu/index.php/meetings/item/15-netiquette-and-online-awareness>

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

1. Avoid posting inflammatory or offensive comments online (a.k.a 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.

The Internet provides a sense of anonymity since you often do not see or hear the people with whom you are communicating online. But that is not an excuse for having poor manners or posting incendiary comments. While some users may feel like they can hide behind their keyboard or smartphone when posting online, the fact is they are still the ones publishing the content. Remember – if you post offensive remarks online and the veil of anonymity is lifted, you will have to answer for the comments you made.

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

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 in 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 in your notebook.

I have learned that _____.
I have realized that _____.
I will apply _____.



What I Can Do

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 is not 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

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

2017. <https://techterms.com>. December 30. Accessed February 17, 2021.

<https://techterms.com/definition/netiquette#:~:text=Netiquette%20is%20short%20for%20%22Internet,good%20behavior%20on%20the%20Internet.>

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>.

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

