Lesson 3
Online Safety and Security, Ethics and Netiquettes

LESSON OBJECTIVES

- determine and avoid the dangers of the Internet;
- consider one's and others' safety when sharing information using the Internet;
- consider one's and others' reputation when using the Internet; and
- report cybercrimes to class.

COMMON ISSUES AND CRIMES ON THE INTERNET

Web-based threats, or online threats, are a category of cybersecurity risks that may cause an undesirable event or action via the internet. Regardless of intent or cause, the consequences of a web threat may damage both individuals and organizations. In recent years, the landscape of web threats has grown significantly. Technologies like smart devices and high-speed mobile networks have allowed for an always-connected vector of malware, fraud, and other complications.

Here are some Internet Threats that you should be aware of:

1. **Malware** – stands for malicious software.
    a. Virus – a malicious program designed to replicate itself and transfer from one computer to another either through the Internet or local networks or data storage like flash drives and CD's.
    b. Worm – a malicious program that transfer s from one computer to another by any type of means. Often it uses a computer network to spread itself. For example, the I LOVE YOU worm (Love Bug Worm) created by a Filipino.
    c. Trojan – a malicious program that is disguised as a useful program but once downloaded or installed leaves your PC unprotected and allows hackers to get your information.
    d. Spyware – a program that runs in the background without you knowing it thus called "spy." It has the ability to monitor what you are currently doing and typing through keyboard.
    e. Adware – a program designed to send you advertisements, mostly as pop-ups.
2. **Spam** – unwanted email mostly from bots or advertisers. It can be used to send malware.
3. **Phishing** – Its goal is to acquire personal sensitive information like passwords and credit card details. This is done by sending you an email that will direct the user to visit a website and be asked to update his/her username, password, credit card or personal information.
4. **Hacking -** it is the unauthorized access to or control over computer network security systems or a private network inside a computer for some illicit purpose.
5. **Identity Theft -** is the crime of obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity to make transactions or purchases online.
6. **Plagiarism -** occurs when an author copies the text of another author, word for word, may it be from the internet or from a book without the use of quotation marks or attribution, thus passing it as his or her own.
7. **Cyberbullying -** is the use of technology to repeatedly and intentionally harass, hurt, embarrass, humiliate, or intimidate another person. Examples of cyberbullying include sending hurtful texts or instant messages, posting embarrassing photos or video on social media, and spreading mean rumors online or with cell phones.
8. **Copyright Issues** - *copyright infringement* occurs when a copyrighted work is reproduced, distributed, performed, publicly displayed, or made into a derivative work without the permission of the copyright owner.

Cybercrime Prevention Act of 2012 (Republic Act No. 10175) – The cybercrime law covers all other online anomalies such as identity theft, child pornography, data misuse, cybersquatting, and other computer-related and Internet-facilitated-practices.

Lesson 3
Online Safety and Security, Ethics and Netiquettes

The internet is defined as the *information superhighway*. This means that everyone has access to this highway, can place information, and can grab that information. Any information, even things that you have set privately can be accessed one way or another. That is why social networking sites like Facebook continue to improve their security features. The threat of cybercrime is very real. While you may not experience the threat now, whatever information we share today could affect your future. *Internet ethics* or *netiquette* is a set of rules that determines how to effectively communicate and browse the web.

The following are some of the good practices when using the Internet:

1. Be mindful of what you share online and what site you share it to.
2. Do not just accept terms and conditions; read it.
3. Check out privacy policy page of a website to learn how the website handles the information you share.
4. Know the security features of the social networking site you use. By keeping your profile private, search engine may not be able to scan your profile.
5. Do not share your password with anyone.
6. Avoid logging in to public networks/Wi—Fi. Browsing in incognito (a feature of the browser) or in private mode, will not protect you from hackers.
7. Do not talk to strangers whether online or face-to-face.
8. Never post anything about a future vacation. It is similar to posting "Rob my house at this 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 conflicts.
12. If you have a Wi-Fi at home, make it a private network by adding password.
13. Avoid downloading anything from untrusted website. You are most vulnerable in peer-to-peer downloads (torrents) as the download is not monitored by the site owner.
14. Buy the software; do not use pirated ones.
15. Do not reply or click links from suspicious emails.

ONLINE SAFETY AND SECURITY

The Internet truly is a powerful tool. It can be used to promote your business, gain new friends, and stay in touch with the old ones. It is also a source of entertainment through games and online communities. The Internet is also one of the most dangerous places, especially if you do not know what you are doing with it. When we use our social media accounts let us make it safe.

Retrieved from: http://allhonestreviews.blogspot.com/2018/05/social-media-hacking-social-media.html

How Safe Are You?	
TYPE OF INFORMATION	**RISKS**
1. First Name	There is still a risk in sharing your first name. Chances are that a hacker already knows plenty of stuff about you even if you only give out your first name. You cannot just walk in a room and start introducing yourself to everyone. You do not know whom you can come across.
2. Last Name	If sharing your first name is a small risk, having both your first and last is riskier. You will be vulnerable to being searched for using search engines, which include image search. Matching a name with a face can led to several cybercrimes like identity theft.
3. Middle Name	Sharing your middle name is probably not the riskiest of these shared information but sharing your entire full name would be.
4. Current and Previous School	Most people who steal identities study their subject. They can use this information for verification purposes.

5. Your cellphone number	Your cellphone number should never be posted over the Internet. The Internet is a public place. It is the same as posting your number on a billboard.
6. The name of your father and mother	Risky yet not as risky as posting their full names, especially your mother's maiden name. Many websites require your mother's maiden name as an answer to a secret question whenever you lose your password.
7. The name of your siblings	This is a huge risk, especially if you have younger siblings. Strangers may pretend or use their identity to dupe you.
8. Your address	Giving the Internet your phone number is one thing, giving them your address is a whole other level. It would be much easier for the criminals to find you.
9. Your home phone number	This shared information is riskier than sharing your personal phone number. Scams usually use this information to deceive you, one of which is when a stranger pretends to be your parents or pretends to be you.
10. Your Birthday	Letting people know your birthday is probably a must if you want to get as many gifts as possible. But having this in your profile makes you vulnerable to identity theft.

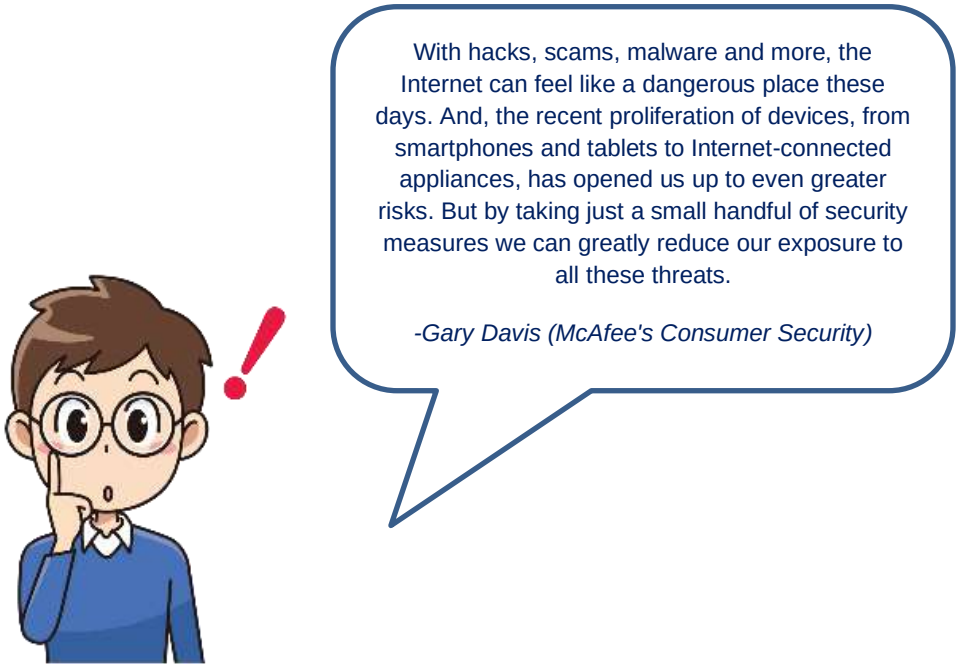
References:

Callo, E. R. (2018). *Science in Today's World for Senior High School Empowerment Technologies*. Quezon City: Sibs Publishing House Inc.

IT Works, Inc. (2018). *Empowerment Technologies Innovative Training Works, Inc*. Manila: Rex Bookstore, Inc.

Melissa P. Juanillo, M. (2019). E-Tech Technology Empowerment in a Connected, Digital World (2nd ed.). (J. D. Ph.D, Ed.) Quezon City: Tech Factors Inc

Yuvienco, J. C. (2016). *Empowerment Technologies for Senior High School (Student Reader)*. Pasig City: Department of Education. Retrieved from: blr.lrqad@deped.gov.ph



Lesson 3
Online Safety and Security, Ethics and Netiquettes

ACTIVITY 3
Cyber News Report

Direction: Form a group with 5-6 members. Research for several news and events related to cybercrime. Choose one (1) issue to present. Using your cellphone or any video-recording device, report it as if you were the newscaster. Assign roles to each member in the group such as reporter, video editor, scriptwriter, and director. Present in 2-3 minutes recording. Submit video in MP4 format.

Cyber News Report Rubric

CRITERIA		SCORE
Content / Organization (8 Points)		
1. Main items in the headline clearly stated and explained; logical, smooth organization.		
2. Clearly, quickly established the focus of the speech, gained audience attention.		
3. Highly detailed, well organized, shows strong research of the issue covered.		
Delivery (8 Points)		
1. Loud, clear, relaxed with few pauses. Well prepared presentation.		
2. Consistent eye contact with many members of the audience; rarely looks at notes.		
Editing (8 Points)		
1. Amount of editing/manipulation is acceptable.		
2. The team has made every attempt to anticipate and filter out unwanted ambient noise in the recording.		
Teamwork (6 Points)		
1. The work done exceeds expectations. Excellent evidence of student learning and efforts are reflected in the project.		
2. Submitted output promptly.		
TOTAL SCORE (30)		

Note: *A time penalty will be given if a team is unable to present all their information within the allotted time.*