Lesson 3.1: Cybersecurity

Objectives

In this lesson, students will:
- ❖ Gain an understanding of the vulnerabilities when on the internet.
- ❖ Learn about specific cybersecurity measures such as strong passwords, data backup and system software updates.
- ❖ Explore applying specific cybersecurity measures to real internet problems.

Agenda

1. Cybersecurity Measures	10 mins
2. Student Activity: The Cybersecurity Report	25 mins
3. Student Activity Solution Discussion: The Cybersecurity Report	15 mins

Resources & Links

- ❏ Cybersecurity Video: https://tinyurl.com/y5dhweo8

Preparation

- ❏ Projector and speakers for video
- ❏ Student activity worksheet printouts, one per student team

1. Cybersecurity Measures

Engage students in an interactive discussion and instruction:

On the internet everything that happens can be seen somehow unless it is protected. That means your personal information, your texts, your emails, your activity. That's why it is important to take steps to keep your data safe. Those steps are called cybersecurity measures.

Let's watch a brief video on cybersecurity:
https://tinyurl.com/y5dhweo8

Student Activity:

Instruct students to briefly discuss with a partner what cybersecurity measures they can take to protect their data when on the internet.

Prompt students for some ideas they came up with, then continue the class discussion and instruction.

Note: It is not necessary to go into detail for each security measure as students will have them available in the student activity.

There are many things we can do to protect our data and personal information. We are going to look at a few simple cybersecurity measures we can do to help keep our data safe.

1. Strong Passwords: A strong password is designed to be complex and therefore difficult to guess or crack. Passwords should also be kept safe and not shared. A strong password has these characteristics:
    - Must be 8 characters or longer
    - Use a combination of upper and lower case letters
    - Use at least 1 numeric or special character (@,%,? etc), punctuation or space

2. Data Backups: A data backup means you copy your data to another location, like a pen drive or another machine. If your data is ever lost, you can restore it from your backup.

3. Software Updates: System updates are received periodically for software. For example, you may receive an update for your online game because new features are developed (for example Minecraft). Sometimes, bad hackers are able to get into your computer

and infect your programs and then they ask you to pay them money to get your computer fixed. This is called *ransomware* and it is illegal but people do it. Making sure that your programs are up to date with the highest level of protection can prevent ransomware.

2. Student Activity: The Cybersecurity Report

In this activity students are presented with a scenario and prompted to engage in a set of reflections and questions about it.

Read the following scenario aloud to the class:

Ana worked on a school report for 6 hours 2 weeks ago. The report is due tomorrow, and she has to add a couple of things before turning it in. She grabs her laptop and rushes to her room to work on it. Boom ! The laptop falls to the floor!   "Oh no !" she says. "But I'm sure everything is ok," she adds. She opens her laptop and looks for her files, but she cannot find any of her files. All her data appears to have been lost in the fall.

Ana is very upset, but then remembers she sent her report via email to a friend Ting just this morning. Thank goodness!   She logs into her email account signing in with her cool password "blahblah" and looks for the email she sent. There is only 1 email in her inbox from her email provider. It says: "We are sorry, your account was logged into by a hacker and they erased all your emails. We will restore all your email up to yesterday. Unfortunately, today's emails were not backed up yet by the provider."   Yesterday ! She calls her friend Ting who uses the same password, well, because they are friends, and finds out that her email account was hacked as well. "Oh no, the report is gone,'' she exclaims. "This is the worst computer day of my life. But I'm sure my teacher will understand I need another week to write my report on cybersecurity".

Explain the activity to students and distribute the activity worksheet. It is recommended that students work on teams for this activity.

3. Student Activity Solution Discussion: The Cybersecurity Report

When students have completed the activity, engage them in a class discussion of the activity questions and answers.

Question	Answers/Discussion Points
What could Ana have done to avoid losing her report and her data? (other than not dropping her laptop :-)	She could backup her data regularly.
What could Ana have done to help guard against a hacker getting into her email account?	She could have used a strong password and kept it safe.
Why is it not a good idea for Ana and Ting to share the same password?	Passwords should always be kept safe and not shared with anyone. If 2 people have the same password, there are twice as many times and places it can be hacked and twice as likely to be misplaced. Even more important though is to not use the same password for different accounts or web sites. Why? Because hackers know people do this. As soon as they hack into the site or your data and get your password, they will go to your next account and try that password.
Let's help Ana come up with 2 ideas of a secure password.	Any combination that makes up a strong password.
When prompted for a valid software update, what should Ana do?	When prompted for a valid software update, particularly of the operating system, one should always perform the update as soon as possible. What do we mean by valid? We need to make the security update from a trusted source. Never click on a link from a text or email to update software unless you are completely sure it is from the software company that owns the app.

Student Activity: Cybersecurity

Read the story aloud with your team (unless everybody remembers everything):

> Ana worked on a school report for 6 hours 2 weeks ago. The report is due tomorrow, and she has to add a couple of things before turning it in. She grabs her laptop and rushes to her room to work on it. Boom ! The laptop falls on the floor! "Oh no !" she says. "But I'm sure everything is ok," she adds. She opens her laptop and looks for her files, but she cannot find any of her files. All her data appears to have been lost in the fall.
>
> Ana is very upset, but then remembers she sent her report via email to a friend just this morning. Thank goodness! She logs into her email account signing in with her cool password "blahblah" and looks for the email she sent. There is only 1 email in her inbox from her email provider. It says: "We are sorry, your account was logged into by a hacker and they erased all your emails. We will restore all your email up to yesterday. Unfortunately, today's emails were not backed up by the provider." Yesterday ! She calls her friend Ting who uses the same password, well, because they are friends, and finds out that her email account was hacked as well. "Oh no, the report is gone'', she exclaims. "This is the worst computer day of my life. But I'm sure my teacher will understand I need another week to write my report on cybersecurity".

Let's help Ana avoid these problems in the future. Read the cybersecurity measures aloud with your team and then decide if any of them could have helped Ana avoid "..the worst computer day …" . Then answer the questions below.

Cybersecurity Measure	What it Means
Strong Passwords	A strong password is designed to be complex and therefore difficult to guess or crack. Passwords should also be kept safe and not shared. A strong password has these characteristics: 1. Must be 8 characters or longer 2. Use a combination of upper and lower case letters 3. Use at least 1 numeric or special character (@,%,? etc), punctuation or space

Data Backup	A data backup means you copy your data to another location, like a pen drive or the cloud. If your data is ever lost, you can restore it from your backup
System Updates	System updates are received periodically for software. They provide new features but often provide fixes to security flaws and hackers love security flaws. Security flaws are responsible for hackers stealing personal information, erasing data and infecting a system with ransomware. Ransomware is software that can threaten to publish personal data or lock a company's system unless money is paid.

1) What could Ana have done to avoid losing her report and her data? (other than not dropping her laptop :-)

   _____

   _____

2) What could Ana have done to help guard against a hacker getting into her email account?

   _____

   _____

3) Let's help Ana come up with 2 secure passwords.

   Password 1:_____

   Password 2:_____

4) Why is it not a good idea for Ana and Ting to share the same password?

_____

_____

5) After Ana's terrible experience, she changed her password and learned how to backup her data regularly.
When she was working on her makeup report, the following message popped up on her screen:

Updates Available
Do you want to install the updates now or try tonight?

Install

Later
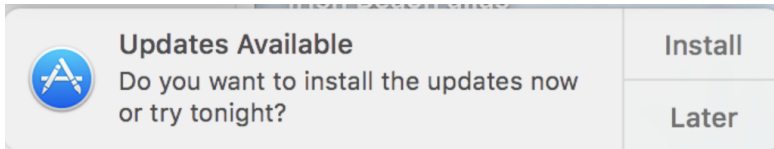
What should Ana do? Keep working since the report is already late? Or ?

_____

_____