Cybersafety Lesson Plan

Grade: 1-4	Subject:	Date:
Topic: **Passwords**	Lesson Title: **Protect Your Candy!**	

Lesson Focus and Goals:

- **Enhance Digital Literacy Skills to Foster Safe Online Practices**
  - create and manage strong passwords, the importance of cybersafety, and recognize common online threats such as phishing and scams.
- **Promote Critical Thinking and Problem Solving**
  - think critically about the consequences of online actions

Materials Needed:

- printed copies of the boardgame and dice (1 per every 2 to 4 students)
- game pieces/markers (1 per student)
- whiteboard/paper and markers to capture discussion points

Structure / Activity: (50 mins)

- conduct the lesson intro discussion **(10 mins)**
- handout copies of the gameboard and play the game in small groups **(10 mins)**
- conduct the discussion scenarios as a large group or smaller breakout groups **(15 mins)**
- review the findings and capture the best practices into a classroom resource (slide/poster) as a large group or smaller breakout groups **(15 mins)**
- optional extensions:
  - share the tip sheet with other classrooms
  - read the tips on the school announcements to share with all students
  - have students take copies home to “teach” their parents and family members
  - allow more time to continue playing the boardgame

Assessment:

- Ask the students to document their answer:
  - Make up a secure password to protect something that is really important to you
  - Write 3 reasons why your password is strong

Cybersafety Lesson Plan

Topic: **Passwords**	Lesson Title: **Protect Your Candy!**

Lesson Introduction Discussion: (10 mins)

Pose the Questions:

- You were given candy and you want to keep it safe - would you lock it in a safe that requires a code with 1 number to open it or needs 3 numbers to open it? How about 9 numbers to open it? - why? what makes it stronger?
- What are some other items you might want to keep safe? (i.e.: bike, scooter, phone, iPad/tablet, $, etc.)?
- How do you protect those items? (i.e.: put in the garage at night, lock it up, leave it at home, etc.)
- What are some items that you own that you can't physically lock up?
  - What about your name? Your email address? Pictures of you? Your voice? Your fingerprints? Your school grades? Information about your health?
  - Where are some of these things stored/kept?
  - Do you have any online accounts? Games - Prodigy, Roblox, Minecraft, Valorant, apps - Spotify, social media accounts - Snapchat, WhatsApp, Instagram, school accounts - Google Classroom, Edbsy, IXL, Raz Kids, etc.
  - What do you have in those accounts that could be lost if someone got into your account? (i.e.: points, skins, armor, your name, address, school, classroom, your friends' names, email address, chat history? etc.)
  - What protects your account and keeps others from getting in?
    - Your Password!

- **Explain** that you are now going to play a game related to passwords and how to make them as strong as possible.

- **Handout** the game materials and review the rules

- **Read** the safeguards and pitfalls on the gameboard and review any words students aren't familiar with
  - Ask students to search online for the definition of any new terms and discuss (see sample definitions/vocabulary sheet below)

- **Play Game (10 mins)**

Cybersafety Lesson Plan

Topic: **Passwords**	Lesson Title: **Protect Your Candy!**

Scenario Discussion Points: (15 mins)

- **Scenario on Reusing Passwords:**
  - **Question**: "Imagine you used the same password for your online game and email. What could happen if someone guessed your game password?"
  - **Purpose**: This scenario helps students consider the risks of password reuse across multiple platforms. The discussion should guide them to understand how a breach in one less secure site can compromise more critical accounts.
- **Scenario on Simple Passwords:**
  - **Question**: "What do you think could happen if you used a password that was really easy to guess, like your pet's name combined with your birth year? Have you or someone you know ever experienced an issue with a simple password like this?"
  - **Purpose**: This encourages students to reflect on the vulnerability of using easily guessable passwords and relate personal experiences where such passwords may have led to security issues.
- **Scenario on Phishing Attempts:**
  - **Question**: "Have you ever received a strange message or email asking you to log in to your account or confirm your password? What did you do about it, and why do you think someone would send these messages?"
  - **Purpose**: Students can discuss experiences with potential phishing attempts and learn to recognize such threats. This helps them understand the importance of verifying the authenticity of requests for sensitive information.
- **Scenario on Password Sharing:**
  - **Question:** "Imagine you let a friend use your login to watch a movie on your account. What might happen if they shared your password with others? How would you handle it?"
  - **Purpose:** This encourages students to consider the consequences of sharing passwords even with trusted friends and discusses the potential ripple effects if the password were to be shared further.
- **Scenario on Secure Recovery Options:**
  - **Question**: "If you forgot your password for a favorite website and needed to reset it, how would having a backup email set up by your parents help you regain access safely?"
  - **Purpose**: This scenario can help students grasp the significance of secure account recovery options, such as parent-managed backup emails, and why it's safer than other less secure methods.

Cybersafety Lesson Plan

Topic: **Passwords**	Lesson Title: **Protect Your Candy!**

- your classroom password best practices should include most/all of the following
- be sure to come up with a clever name and eye-catching design!

Ms. Connor's **Cyber Savvy Superstars:**

Our Classroom Guide to Passwords

- **Use Passphrases**: Start with a passphrase which is easy to remember but hard to guess, such as "BlueBananaDancesInTheSun!"
- **Make it Long and Complex:** at least 12 characters long and include uppercase and lowercase letters, numbers, and symbols: "Blu3BananaDances1nTheS@n!45"
- **Never Reuse Passwords**: Each account should have its own unique password.
- **Keep Passwords Secret:** Never share passwords, not even with close friends.
- **Use a Password Manager:** To create, store and manage all passwords securely. Note: young students may require parental assistance.
- **Enable Two-Factor Authentication (2FA)**: A code sent to a phone or email, can protect your account even if someone else finds out the password.
- **Avoid Personal Information**: Don't use easily known or guessed information such as names, birthdays, or addresses in passwords.
- **Never Enter Passwords in Pop-ups:** Safe websites and apps will not ask for passwords through pop-up windows.
- **Don't Share Passwords for Prizes or Gifts**: Real contests or games will require your password.
- **Be Wary of Emails or Messages Asking for Passwords**: Never type your password into websites or forms accessed through links in emails or messages.
- **Use Parent-Managed Backup Email for Account Recovery**: Set up online accounts with a parent's email as a backup for password recovery and account verification. This allows parents to help securely reset passwords or verify account ownership if there are any suspicious activities.

Cybersafety Lesson Plan

Topic: **Passwords**	Lesson Title: **Protect Your Candy!**

Definitions/Vocabulary

- **Password:** A secret word or phrase that you use to get into your accounts on the computer, like your email or games. Only you should know it.
- **Complex Password:** A password that includes lots of different types of characters, like big letters, small letters, numbers, and special symbols (like !, @, #). This makes it hard for others to guess.
- **Password Manager:** A special program that keeps all your passwords safe in one place. It can also help you make new, strong passwords.
- **2-Factor Authentication (2FA):** A way to keep your account extra safe by using two different checks before you can log in. Usually, it's your password and then a code sent to your phone or email.
- **Pop-up:** A small window that suddenly appears ("pops up") on your computer screen, often when you are browsing the internet. Sometimes they are advertisements or important messages, but sometimes they can be tricks.
- **Reused Password:** Using the same password for different things, like your game account and your email. This isn't safe because if someone finds out your password in one place, they can get into your other accounts.
- **Default Password:** The original password that comes with a device or account when you first get it. You should change this to a password that only you know.
- **Personal Information:** Details about you, like your name, where you live, or your birthday. You shouldn't use this in your passwords because someone who knows you might guess it.
- **Phishing:** A trick where someone tries to get you to give them your personal information, like your password, by pretending to be a trustworthy person or company in an email or other communication.

Cybersafety Lesson Plan

Topic: **Passwords**	Lesson Title: **Protect Your Candy!**

Additional Curriculum Links:

1. **Digital Literacy and Information Technology**
   - **Learning Outcome**: Understand the basics of digital citizenship and safe internet practices.
   - **Curriculum Connection**: Many Canadian provinces include digital literacy from an early age. For example, in Ontario, the curriculum covers safe and responsible use of digital tools. Discussing password security and the consequences of sharing personal information can help meet these outcomes by teaching students how to navigate online spaces responsibly.
2. **Critical Thinking and Problem Solving**
   - **Learning Outcome**: Develop critical thinking skills by evaluating information and making informed decisions.
   - **Curriculum Connection**: Critical thinking is emphasized across Canadian curricula. By analyzing scenarios like ignoring pop-ups or not reusing passwords, students practice decision-making and learn to identify trustworthy sources of information.
3. **Personal and Social Development**
   - **Learning Outcome**: Foster personal responsibility and ethical decision-making.
   - **Curriculum Connection**: This area is often covered under health and personal development subjects. Discussing scenarios such as not sharing passwords even with friends supports learning about boundaries and ethical behavior in personal interactions, especially relevant in Alberta's and British Columbia's curricula, which emphasize personal responsibility.
4. **Language Arts**
   - **Learning Outcome**: Enhance communication skills by discussing and articulating thoughts and ideas clearly.
   - **Curriculum Connection**: Engaging in discussions about digital safety scenarios helps students practice expressing their thoughts, asking questions, and presenting ideas clearly, directly supporting language arts goals in all provinces.
5. **Mathematics and Logical Reasoning**
   - **Learning Outcome**: Apply logical reasoning to solve problems and understand patterns.
   - **Curriculum Connection**: Discussing the impact of the number of possible combinations based on the length and mix of characters and symbols and related probabilities of guessing on password strength can help students apply logical reasoning, a key component of the math curriculum.