Activity 2 : Create a good password and how to manage it

Objective of Activity 2

Understand why it is important to use a good password and know the basic rules for having a strong password.

Soft Skills to be Acquired in Cyber Security

Resourcefulness, observation and critical thinking.

Please Note

All of our activities can be done during class time and can be inserted into the teaching of your different programs of study. For example, reading the article could be seen as an activity in an English class and using the micro:bit as a cross-curricular activity in technology.

Useful Glossary for This Activity

- **Key**: This is the code for decrypting information sent in a message.

- **Encryption**: The act of converting information into a code that makes it difficult or impossible to read.

- **Strong password**: A password with features that make it secure and difficult to guess or find.

- **Password dictionary**: A way for hackers to try multiple passwords quickly to detect accounts that use a weak password.

- **Password manager**: Software that can be installed that encrypts your password information and allows you to use it whenever you need it.

- **Two-step authentication**: This is the act of identifying yourself twice in two different ways to authenticate who you are.

- **Weak password**: A password that is easy to detect and does not contain many letters, numbers and special symbols.

Before the Activity Begins

Make sure you have the necessary materials and tools on hand before the students arrive. Decide on the best way to distribute the materials. Don't hesitate to ask your students to help out. Why not appoint one or two students to be responsible for preparing the materials before the activity is presented? We suggest teams of 4 or 5 students for this activity.

Materials required from the kit

The kit contains several types of materials that will be used throughout our activities. It is not necessary to have everything available for the students. This is at your discretion. Some teachers may prefer to make only the required materials available to students and others may consider full access to the kit by students. For Activity 2, you will need the following materials:

- 1 micro:bit per team;
- 1 b.Board per team;
- 1 USB cable per team;
- 1 computer with internet access per team.
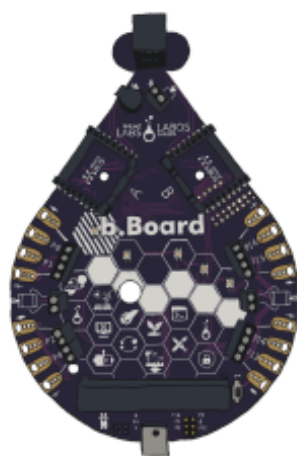
b.Board
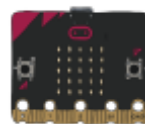
micro:bit
(V1 or V2)

Part 1 - Activity with the micro:bit: Make a Blixel light up

The micro:bit is a powerful micro controller and you will have the chance to try coding activities that will give you a better understanding of how to protect yourself and how the world of cyber security works. We will walk you through the steps and you can give students time to explore and try to create their own programs. This activity will allow students to light-up the micro:bit's display with their community's name. They can take the name of their community or start thinking of a name they would like to use for building their smart community later in the other activities.

Preparation and instructions for connecting the micro:bit and the b.Board to your laptop
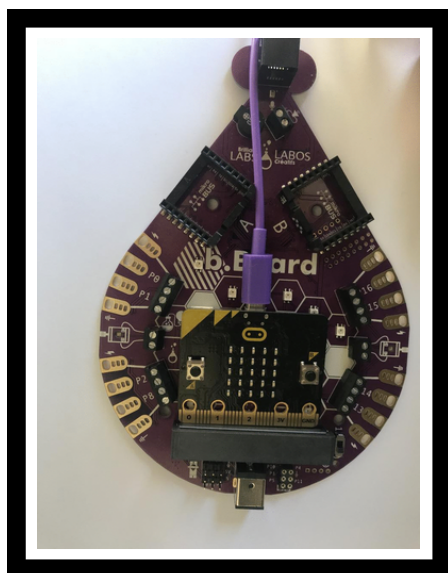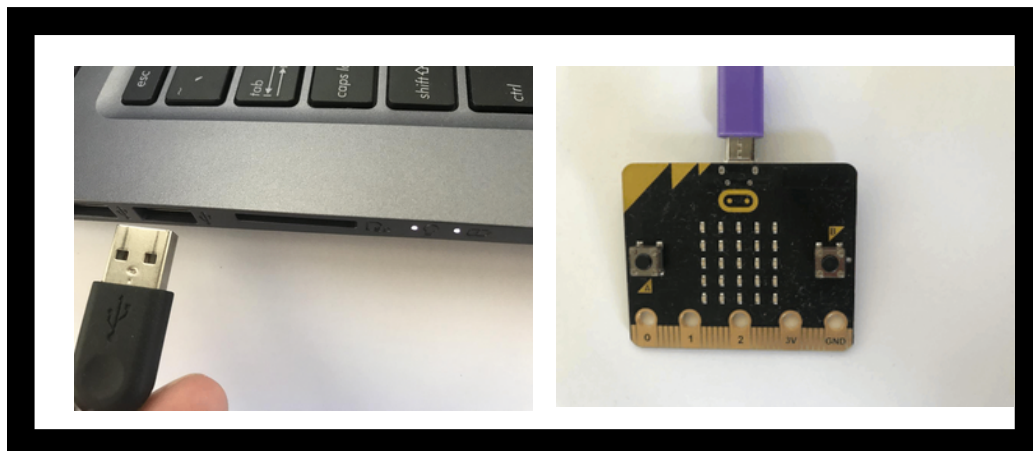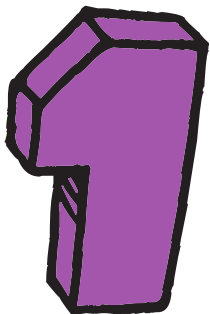
Connect the USB wire to the computer (not an iPad) and the other end of the wire into the micro:bit. If you want to use a tablet you can download the micro:bit app and flash the code.brilliantlabs.ca file via bluetooth.

Insert the micro:bit into the B.board. and ensure the bottom row of the Micro:bit pins are completely instered.
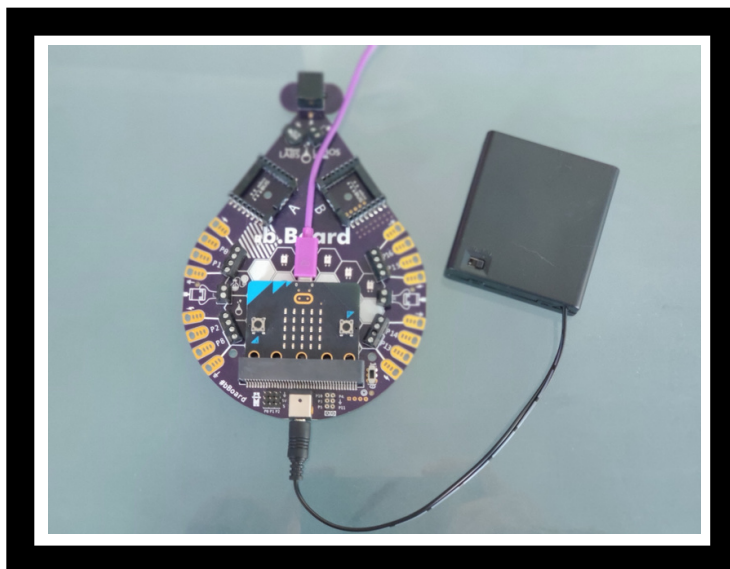
**Preparation and instructions for connecting the micro:bit and the b.Board to your laptop**

3

Connect the battery pack and if your pack has an on/off switch please ensure to turn on the battery pack. (Please note there are various wall chargers and battery pack that function with the b.Board so yours may look different than the picture above.

4

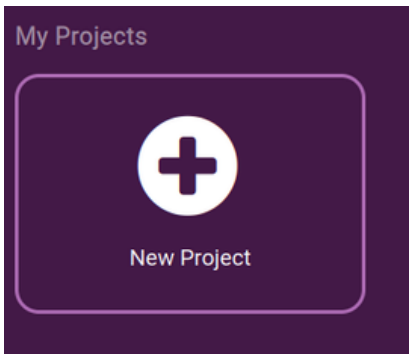With everything connected it is now time to turn on the b.Board using the on/off switch next to the micro:bit connector.
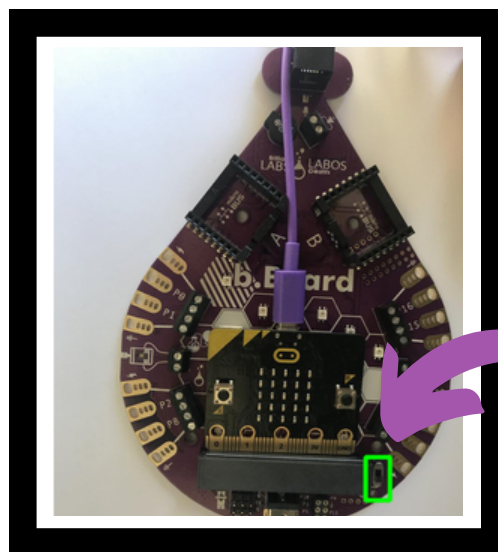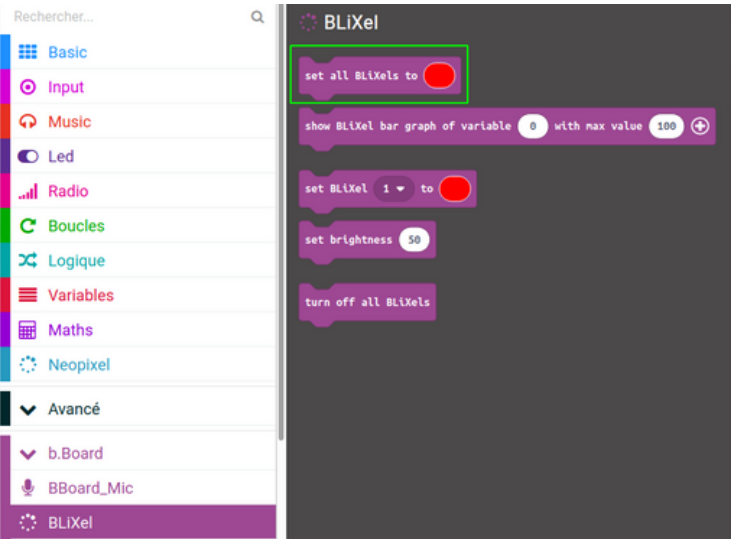
Let's start Activity 2

To access the portal go to
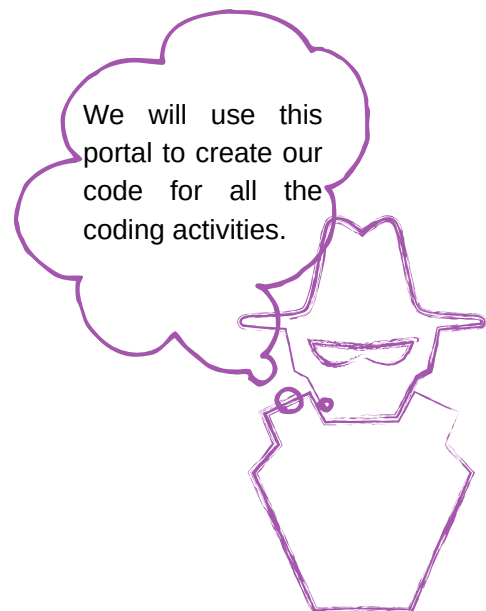https://code.brilliantlabs.ca

Start a new project by giving a name to your activity (ie: Activity 2).

We will use this portal to create our code for all the coding activities.

In the section **b.Board**, under **BLiXel**, drag the block **Set all BLiXels to** in the block **forever**

3

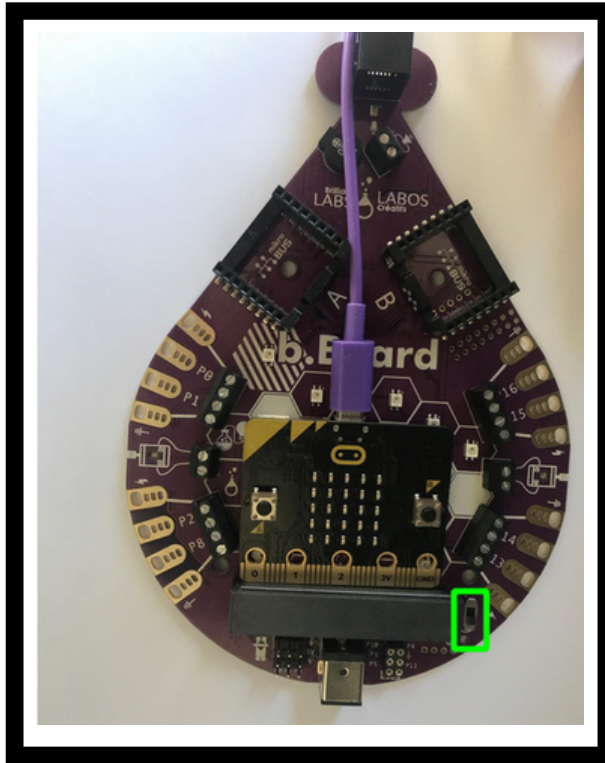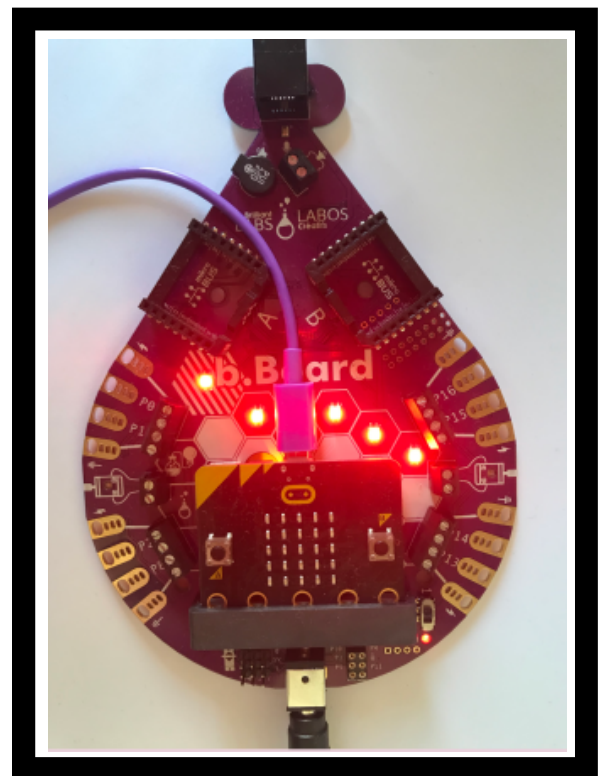Now save your .hex file into the micro:bit and make sure your b.Board is turned on.

4

BliXel lights up in red.
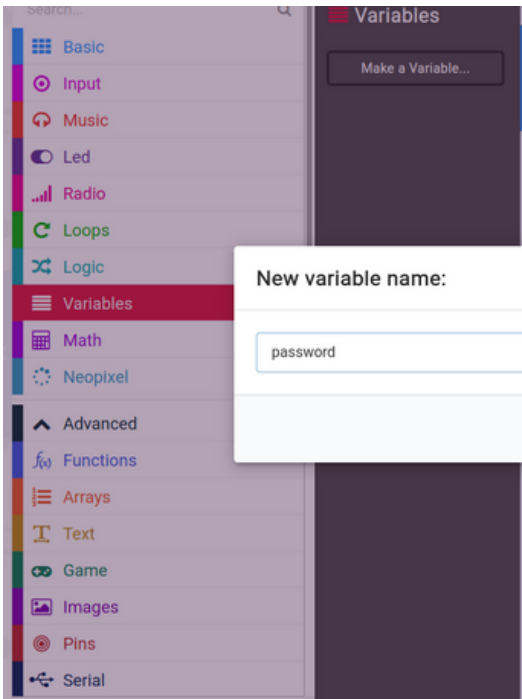
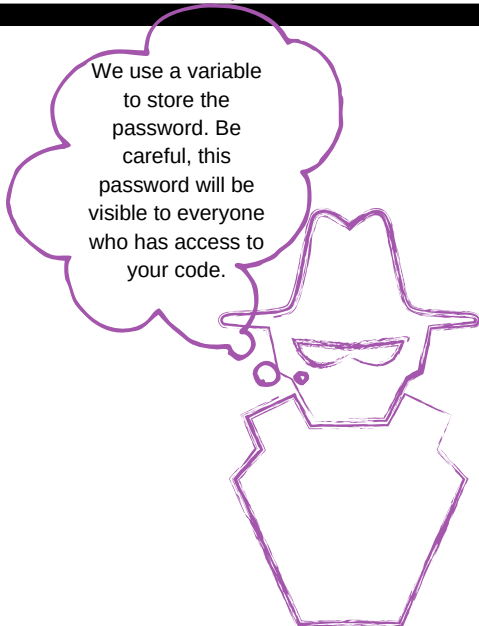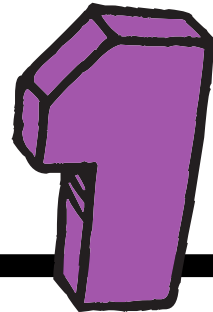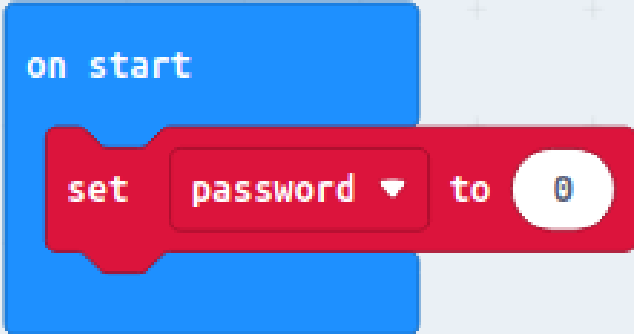## Light up the BliXel According to a Specific Password

In the section **Variables**, create a new variable named password.

We use a variable to store the password. Be careful, this password will be visible to everyone who has access to your code.

Bring the block **Set password to 0** in the **On start** block.

Now you need to adjust the block to accommodate a password containing letters and numbers.

In the Advanced section, under Text, move the quotation marks in the block to replace the number 0 with the quotation marks

Now you need to adjust the block to accommodate a password containing letters and numbers.

3

In the Advanced section, under Text, move the quotation marks in the block to replace the number 0 with the quotation marks

After that, all you have to do is choose your password.

Now you have to tell the micro:bit to turn on the lights if the password is correct. In the Logic section, move the if-else block to the Forever block.

In the Logic section, bring the quotation marks to replace the True condition.
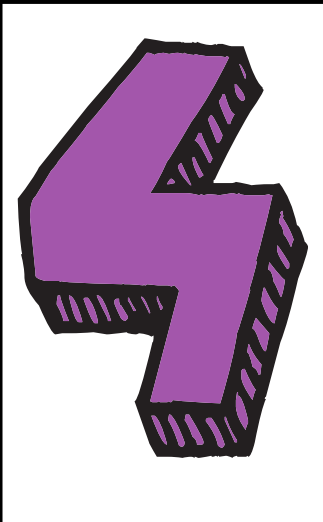
All that remains is to compare the password variable with the desired password and to specify what would happen if the password is correct and if the password is not correct.

Always remember to save your .hex file into the micro:bit and make sure your b.Board is turned on every time you make a change to your code!

Explanation

We started by creating a variable named password and placed it in the block startup by assigning it the value 123456. This tells the micro:bit to create the variable and assign the text 123456 to it as soon as the micro:bit is started.

Afterwards, we inserted a little logic in the forever block in order to specify to the micro:bit what would happen if our variable did not have the same value as the password assigned to our logic. If the password of our variable password (which is created at startup) is equal to the text 123456, then the lights turn on green. Otherwise, the lights will turn red. Try changing the password in one place and see what happens.

Suggestions for going further with your micro:bit

- Try to find and see the source code of your program on the website.
- Try to change the code blocks to add or change the way the program works.

Let's go further

To finish this first part, we invite you to download the following hex file in your micro:bit. The file may have been created by a hacker... Will you dare to start your b.Board anyway? What do you think about it? This is what we will discuss in the next part...

[HEX file to download](#)

End of Part 1
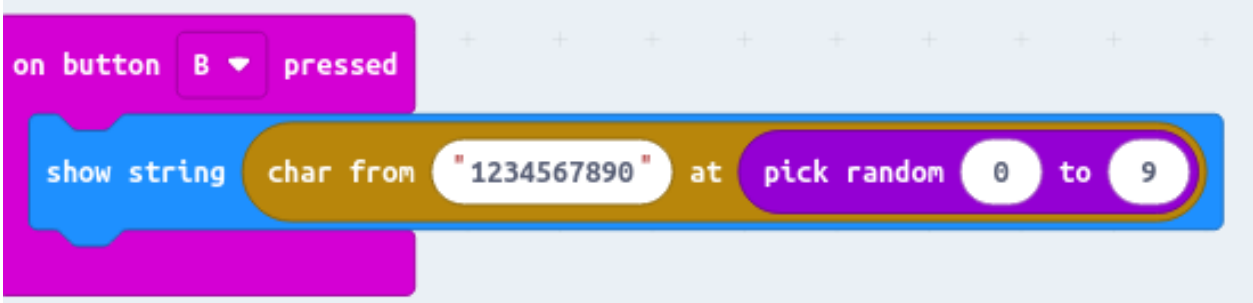
What if you could generate a password with the micro:bit?
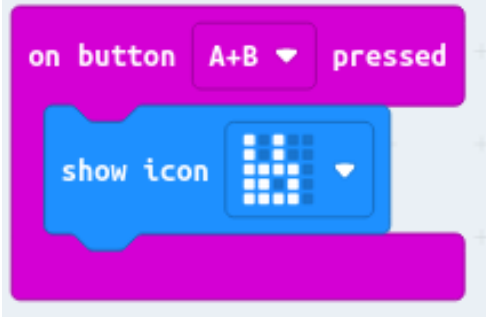
Here's some steps you could follow to generate a password. For this activity, let's assume we want to generate a password with characters and numbers with a total length of 12. Use a pencil to write down the letters and numbers on a piece of paper. When you have 12 characters, stop.

When we press button A, the micro:bit will randomly select a character between the range of characters we specified.
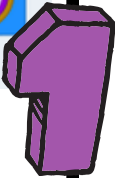
When we press button B, the micro:bit will randomly select a number between 0 and 9.

What do you think about the idea of storing your password on a piece of paper?

When we press buttons A+B together, the micro:bit will show a little image.

Part 2 - Cyber Security Activity: Online Password 123456

Read with students the article "Online password '123456' more popular than ever and easy to crack" from the CBC website.

Source: https://www.cbc.ca/news/business/nordpass-list-of-most-common-and-worst-passwords-1.5807089

Maker of password manager app details worst passwords of 2020

CBC News · Posted: Nov 18, 2020 4:48 PM ET | Last Updated: November 18, 2020

Discussion with students following the reading of the article

- What do you remember from reading this article?
- Why do people choose a weak password?
- What would a strong password be?
- What are the risks of using a weak password?
- What are some tips for having a strong password?

Suggestions for possible follow-up activities to do in class

- Write a letter to an adult explaining the importance of passwords.
- Make a pamphlet about the importance of passwords.
- Make a poster on how to have a strong password.
- Make a video about the importance of passwords and how to protect yourself.
- Conduct a survey on the types of passwords used by students and/or adults.
- Make a vox pop about password use in your school.
- Make a podcast about the importance of passwords.

Links of Websites to go further with this activity

Please note that since the links below come from a third party, Creative Labs is not responsible for its content or for any suggested links published by them. We strongly suggest that you take the time to go through each of these links before using them and to ensure that they are in line with your values and what you normally use in class with your students.

- Article, CBC: [Netflix testing household-verification feature for shared passwords](#)
- YouTube video: [Get Cyber Safe | Creating a strong password](#)
- YouTube video: [How to Create a Strong Password](#)
- Website: [Strong Password Generator : Stay Safe online](#)
- Website: Have I been Pawned ? To see if your email has been compromise: https://haveibeenpwned.com/
- Website: [Creating Strong Password | Password Tips](#)
- Website: [How strong is your password ? Five ways to evaluate](#)

A moment to think about the activity (We suggest the following questions or create others as needed)

- What did we learn from this activity?
- Why is this important?
- Will you change the way you manage your passwords?
- What advice would you give to someone who uses weak passwords?
- Other questions from the teacher...

End of Activity 2