



BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT



Activity 3: Malware, how to protect yourself

Objective of Activity 3

The objective of this activity is to help you better understand the role of malware in cybersecurity and how to protect yourself. Take the time to read the proposed article and have the kids search the web as needed to determine the meaning of the new words. The activities are always done in 2 parts; one part programming a micro:bit and one part learning about cybersecurity.

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.





BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT



Useful Glossary for This Activity

- **Computer attack:** When hackers have personal information in their possession, they can launch a series of computer attacks. There are attacks that are targeted at specific individuals or mass attacks that are aimed at many people at the same time. Most often, the attack consists of fraudulent e-mails or links to fake websites.
- **Fraudulent e-mail:** This is an e-mail from a dubious source that asks you to open a suspicious link or to send personal information (name, bank account, credit card number, etc.). It is very important to be vigilant because some emails look like real emails from existing companies.
- **Cybercrime:** A criminal activity that targets or uses a computer, computer network or networked device. Most (but not all) cybercriminal activity is committed by cybercriminals or hackers who want to make money. (source)
- **Botnet:** This is a network of hacked computers that allows, for example, to send malicious emails on a very large scale.
- **Social engineering:** This is a tactic to understand how people react to emails or computer links. For example, hackers often use a sense of urgency to get users to click on links quickly without thinking. In this way, they manage to get malware installed on users' devices and can then carry out an attack.
- **Malicious software or malware:** This is a computer program often installed without the users' knowledge, which allows a person to receive confidential information or control a computer remotely. This activity is illegal and allows a hacker to accumulate confidential information and extort money from victims.
- **Attachment:** This is a file that is sent with an email. Unfortunately, some attachments are often malware that users install on their devices. Users install it by clicking on the file to view it.
- **Ransomware:** This is an online scam that allows a hacker to remotely lock down a person's computer and demand an amount of money (ransom) in exchange for a code to unlock the computer. Transactions are often made in Bitcoins.
- **Phishing:** This is a tactic used by hackers to trick us.





BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT



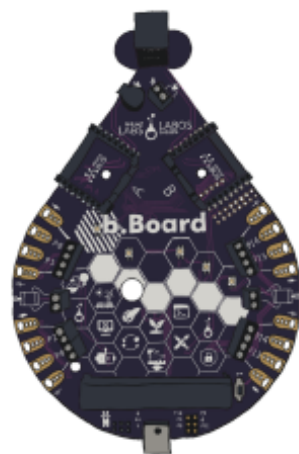
Before the Activity Begins

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 3, you will need the following materials:

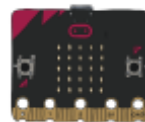
- 1 micro:bit per team;
- 1 b.Board per team;
- 1 USB cable per team;
- 1 computer with internet access per team.



b.Board



Servo



micro:bit
(V1 or V2)





BRILLIANT LABS CYBER SECURITY

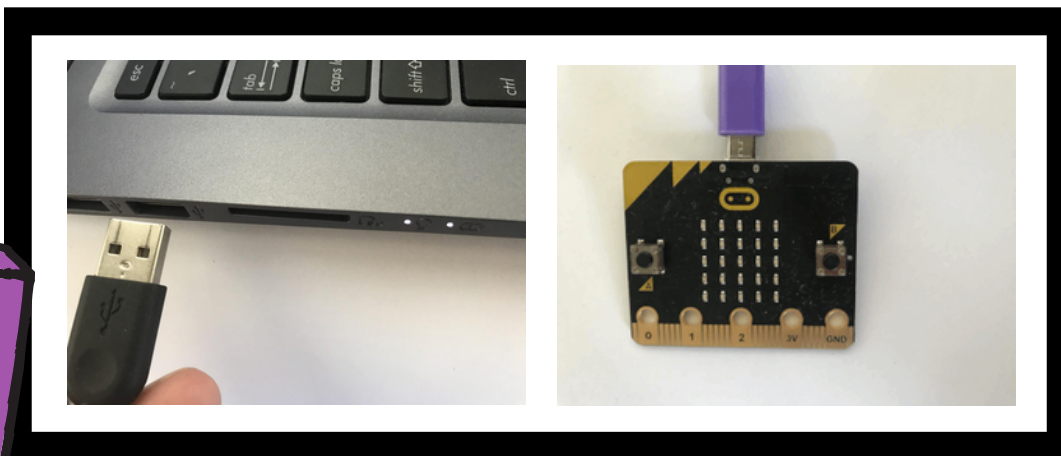
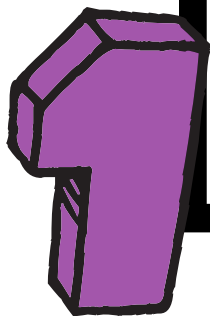
INTRODUCTION KIT



Part 1 - Activity with the micro:bit: Running a servo motor

The micro:bit is a simple computer and you will have the chance to do some 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 this and you can also give students time to explore and try to create their own programs.

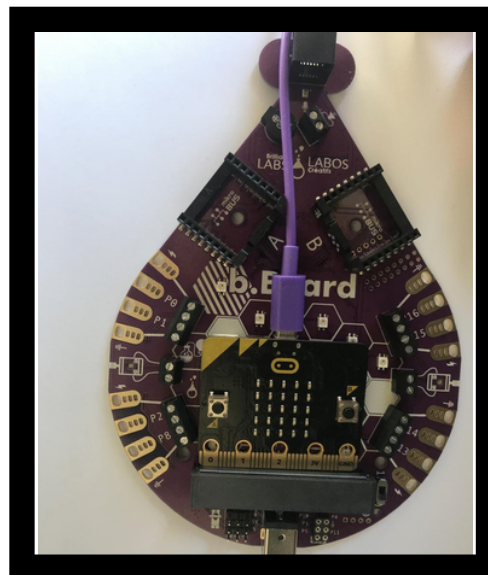
Preparation and instructions for connecting the micro:bit and the b.Board to your laptop



Connect the USB wire to the computer (not an iPad) and the other end of the wire into the micro:bit.



Insert the micro:bit into the B.board firmly and ensure all the pins are well placed inside the b.Board connector. Please note the micro:bit screen needs to face forward.





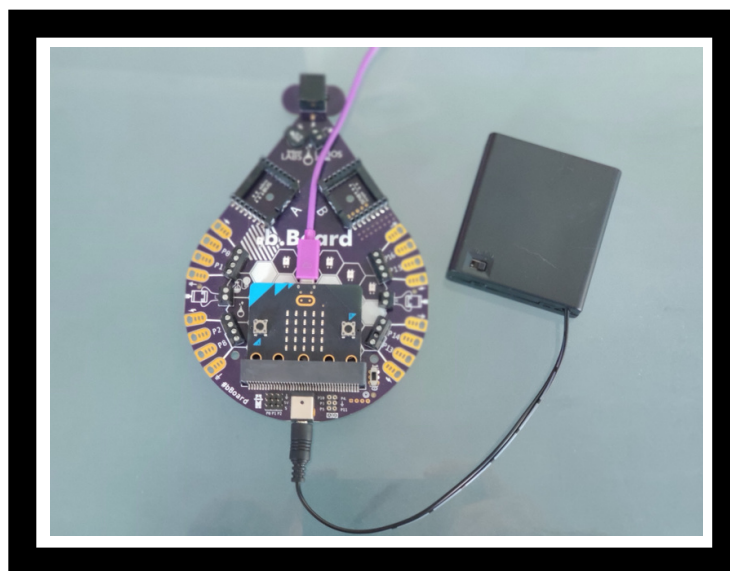
BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT



Preparation and instructions for connecting the micro:bit and the b.Board to your laptop

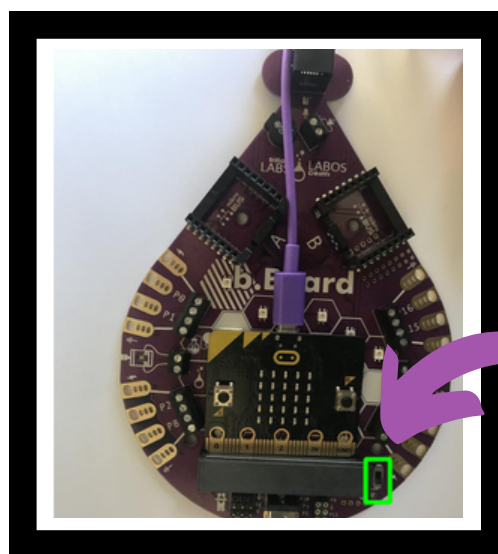
3



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.





BRILLIANT LABS CYBER SECURITY

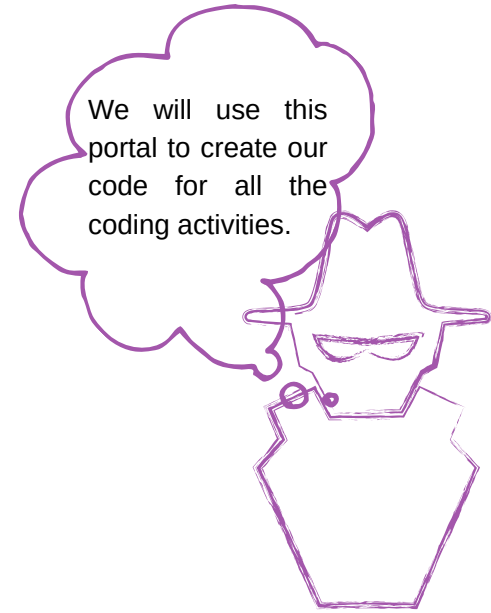
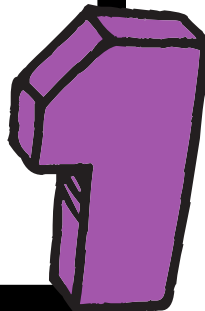
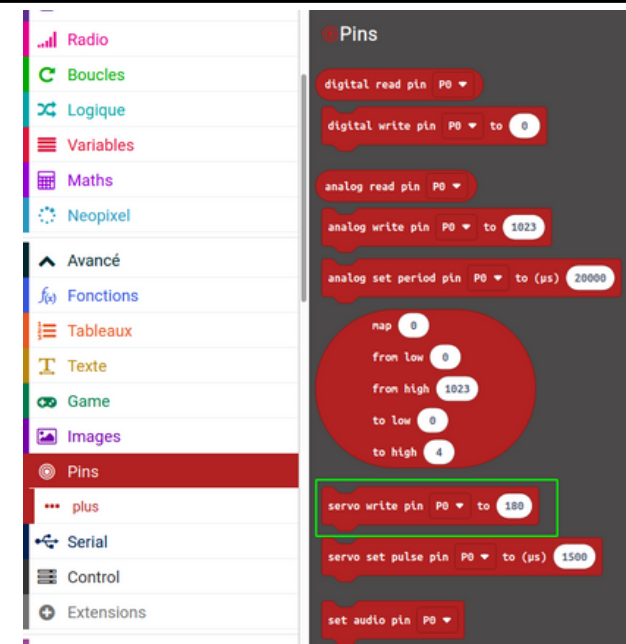
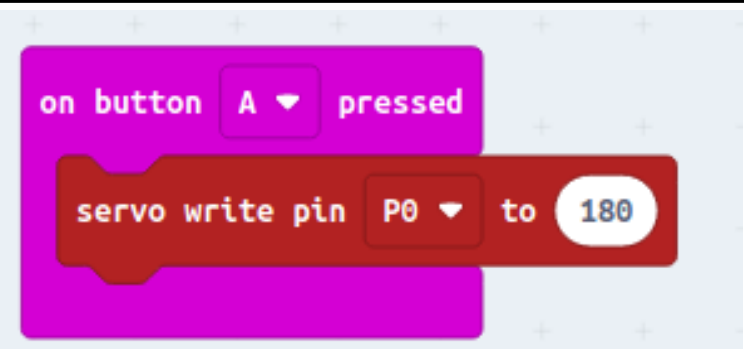
INTRODUCTION KIT



Let's start Activity 3



Go to <https://code.brilliantlabs.ca> and start a new project by giving a name to your activity (ie: Activity 3).

In the **Advanced** section, and under **Pins**, bring the block **servo write pin P0 to 180** in the block **on button A pressed**.





BRILLIANT LABS CYBER SECURITY

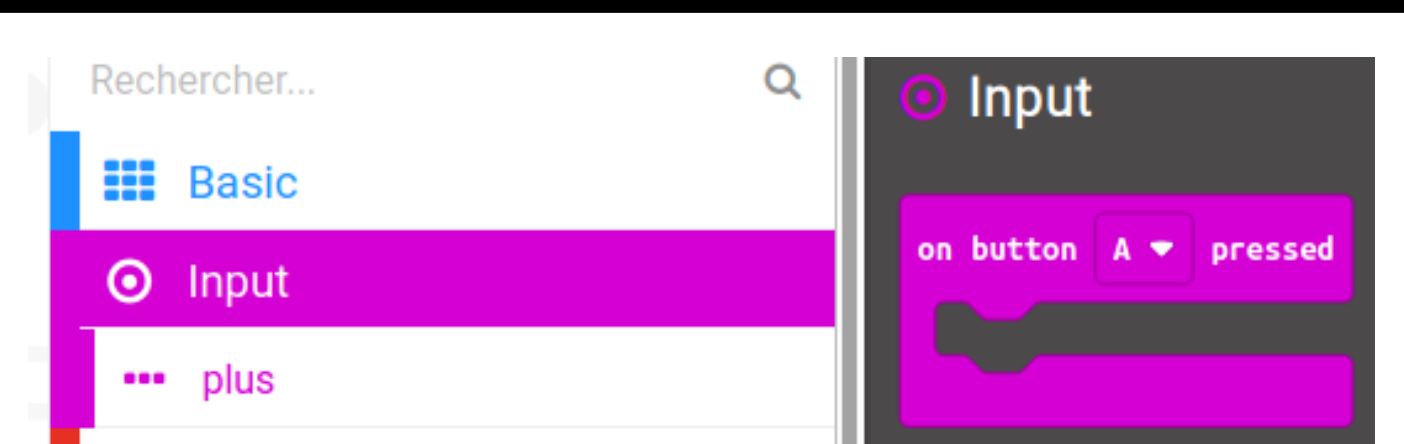
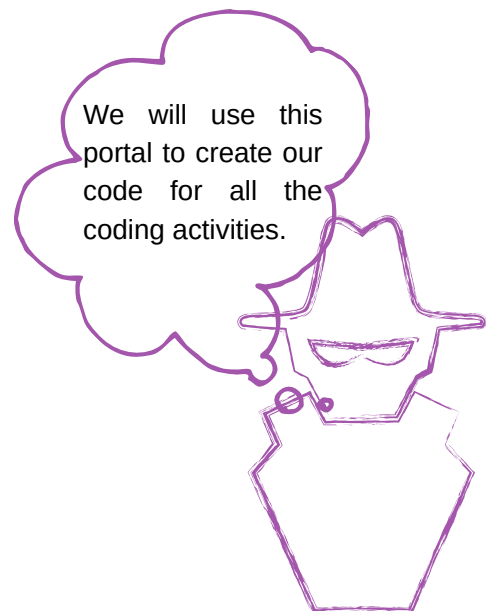
INTRODUCTION KIT




Let's start Activity 3



Go to <https://code.brilliantlabs.ca> and start a new project by giving a name to your activity (ie: Activity 3).



In the **Input** section, bring the block **on button A pressed** on the working area.



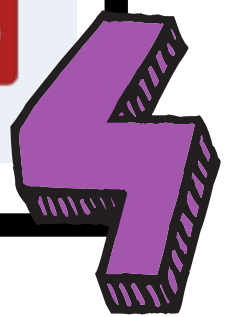


BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT



In the **Advanced** section, and under **Pins**, bring the block **servo write pin P0 to 180** in the block on button A pressed.



BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT



In the **Input** section, bring a second block **on button A pressed** on the work surface. Change A to B



In the **Advanced** section, and under **Pins**, bring the **servo write pin block P0 to 180** into the **on button B pressed** block. Change the value to 0



BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT

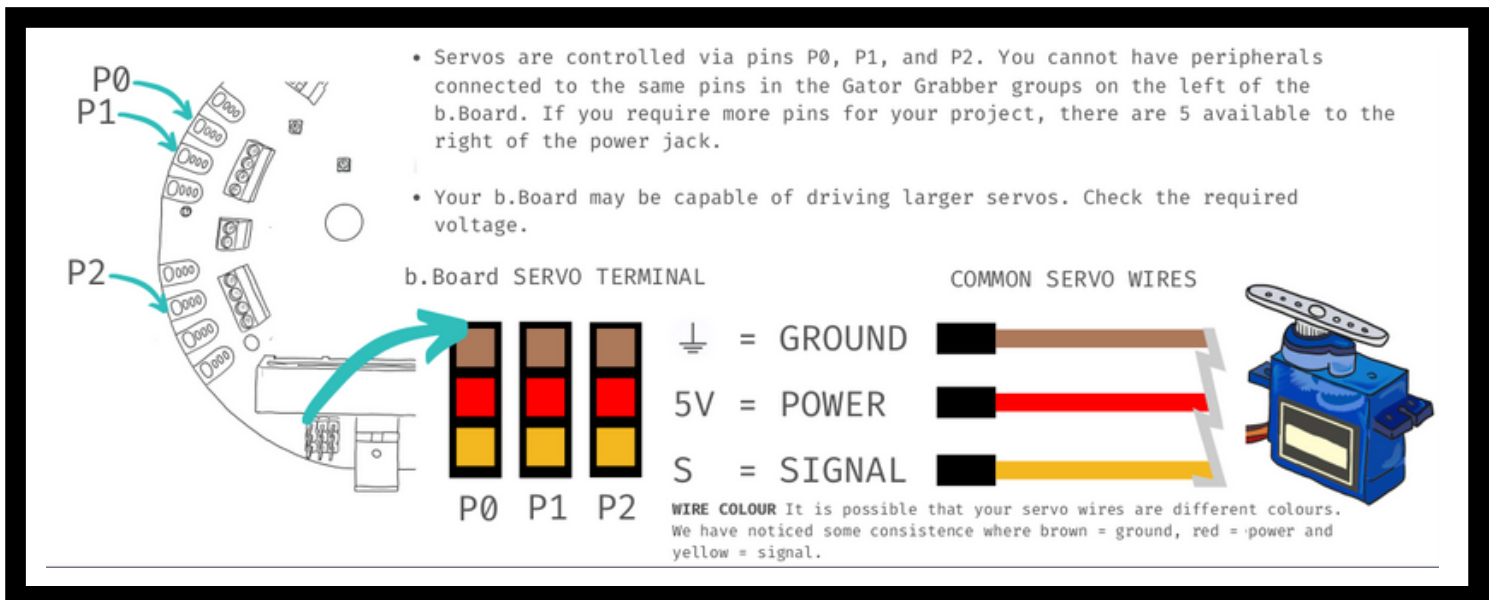
Explanation

The code we have developed allows for 2 possibilities. First, when we press button A, the servo motor will turn 180 degrees.

Secondly, when we press button B, the servo motor will turn in the opposite direction.

How to connect the Servo?

To view the result of this code, you will need to connect your servo motor to the b.Board. The following figure shows where to connect your servo motor.





BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT

How to download your code to the micro:bit?

- Please make sure that your micro:bit is connected to your laptop. Please refer to page 4 if necessary.
- Click on Download and save the .hex file to the micro:bit.
- Press Button A and then press Button B.

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



BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT



Part 2 - Cyber Security Activity International cybercops derail botnet

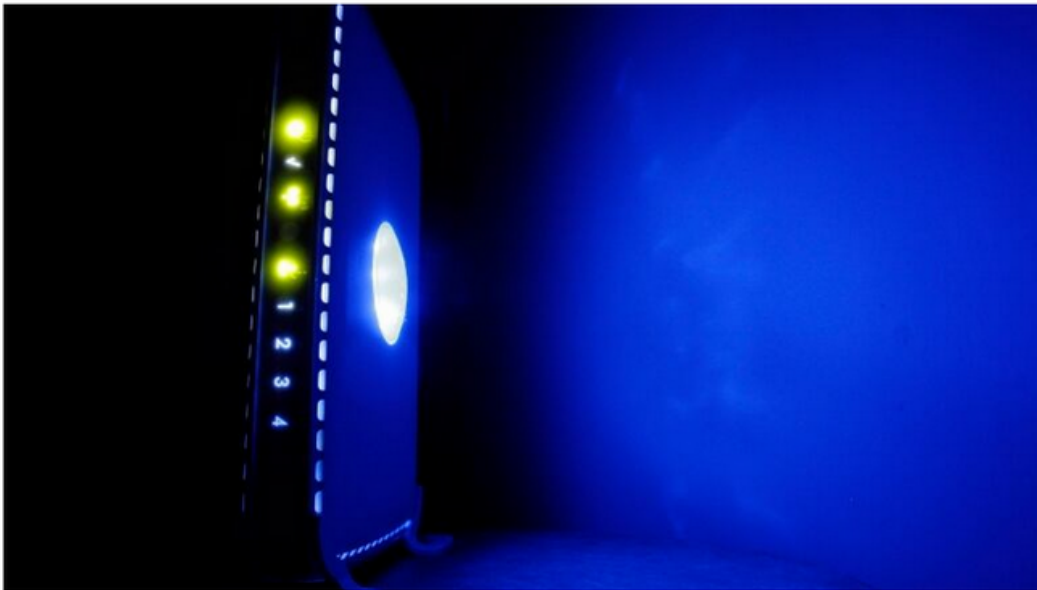
Read, with the students, the article “International cybercops derail botnet used to extort, steal data around the globe for years” from the CBC website.

Link to the article:

<https://www.cbc.ca/news/world/cybercrime-botnet-derailed-canadian-arrested-1.5890484>

FBI also announced the arrest of a Canadian on Wednesday in connection to a ransomware attack

The Associated Press · Posted: Jan 27, 2021 5:16 PM ET | Last Updated: January 27



Global Investigators have disrupted one of the world's largest networks for seeding malware infections that has been used for years to steal data and extort governments, health care and educational institutions. (Matt Rourke/The Associated Press)



BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT



Questions to ask and possible discussion with students after reading the article

- What do you remember after reading this article?
- Why is it important to know how to protect yourself?
- How often do you use email? What are the advantages and disadvantages?
- Have you ever had a bad experience with malware?
- What tips would you give your friends or family members to better protect themselves with malware?

Suggestions for possible follow-up activities to do in class

- Write a letter to an adult explaining the importance of malware.
- Make a flyer about the importance of malware.
- Make a poster on tips to protect yourself from malware.
- Make a video to explain malware and how to protect yourself.
- Make a podcast about the importance of protecting yourself from malware.



BRILLIANT LABS CYBER SECURITY

INTRODUCTION KIT

Suggested links to learn more and to go further with this activity

Please note that the links below are from a third party and Brilliant Labs is not responsible for their content or suggested links published by them. We strongly suggest that you take the time to review each of these links before using them and ensure that they are consistent with your values and what you normally use in your classroom with your students.

- **CBC, News article:** [Hacking attacks on government growing more sophisticated, intelligence agency warns](#)
- **YouTube Video:** [Get Cyber Safe | Malware and Ransomware](#)
- **YouTube Video, Government of Canada:** [Get Cyber Safe | Phishing: Don't take the Bait!](#)
- **YouTube Video, Government of Canada:** [Get Cyber Safe | Phishing Scams](#)
- **Website, Government of Canada:** [What is malware : How to protect yourself](#)
- **Infographic, Government of Canada:** [Malware infographic detected!](#)
- **Website, Brilliant Labs:** [Cyber Security Resource Database](#)
- **Glossary, Government of Canada:** [Cybersecurity Glossary](#)

Objectivation questions to complete the activity

You can also create other questions if you deem it necessary.

- What did we learn from this activity?
- Why is this important?
- Will you put some of the things you learned?
- How can we help reduce the impact of cyber security malware as a 21st century citizen?
- Other questions from the teacher...

End of Activity 3