Activité 3 : Les maliciels, savoir se protéger

Objectif de l’activité 3

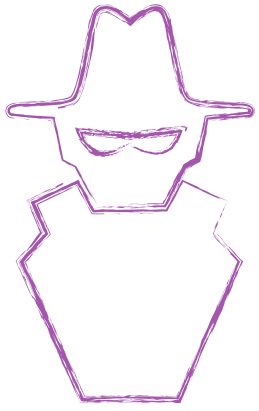
Cette activité a pour objectif de vous aider à mieux comprendre le rôle des maliciels en cybersécurité et de savoir comment se protéger. Prenez le temps de lire l’article proposé et de demander aux jeunes de fouiller au besoin sur le Web afin de déterminer le sens des mots nouveaux. Les activités se font toujours en 2 parties ; une partie de programmation d’un micro:bit et une partie d’apprentissage en cybersécurité.

Compétences non techniques visées en cybersécurité

La débrouillardise, l'observation et la pensée critique.

Veuillez prendre note

Toutes nos activités peuvent être faites pendant le temps de classe et être insérées lors de l’enseignement de vos différents programmes d’études. Par exemple, la lecture de l’article pourrait être vue comme une activité dans le cadre du cours de français et l’utilisation du micro:bit dans le cadre d’une activité transdisciplinaires en technologie.



Glossaire utile pour l'activité 3

- **Attaque informatique** : Lorsque les pirates informatiques ont en leur possession d'informations personnelles, ils peuvent lancer une série d'attaques informatiques. Il existe des attaques ciblées envers des personnes en particulier ou des attaques de masse qui s'adressent à plusieurs personnes en même temps. Le plus souvent, l'attaque consiste à des courriels frauduleux ou a des liens déposés sur de faux sites Web.

- **Courriel frauduleux** : C'est un courriel provenant d'une source douteuse et qui vous demande d'ouvrir un lien louche ou d'envoyer des informations personnelles (nom, compte de banque, numéro de carte de crédit, etc.). Il est très important d'être vigilant car certains courriels ressemblent à de vrais courriels provenant de compagnies existantes.

- **Cybercriminalité** : Une activité criminelle qui cible ou utilise un ordinateur, un réseau informatique ou un appareil mis en réseau. La plupart des activités cybercriminelles (mais pas toutes) sont commises par des cybercriminels ou des pirates informatiques qui veulent se faire de l'argent. (source)

- **Réseau zombie (botnet)** : C'est un réseau d'ordinateurs piratés qui permet, par exemple, d'envoyer des courriels malveillants à très grande échelle.

- **Ingénierie sociale** : C'est une tactique pour comprendre comment les gens réagissent à des courriels ou des liens informatiques. Les pirates informatiques utilisent souvent par exemple un sentiment d'urgence pour faire en sorte que des utilisateurs cliquent sur des liens rapidement sans réfléchir. Il réussissent ainsi à provoquer l'installation de malware sur les appareils d'utilisateurs et peuvent procéder par la suite à une attaque.

- **Logiciel malveillant ou maliciel (malware)** : C'est un programme informatique souvent installé à l'insu des utilisateurs, qui permet à une personne de recevoir des informations confidentielles ou de contrôler à distance un ordinateur. Cette activité est illégale et permet à un pirate informatique d'accumuler des information confidentielles et d'extorquer de l'argent à des victimes.

- **Pièce jointe** : C'est un fichier qui est envoyé avec un courriel. Malheureusement, il arrive souvent que certaines pièces jointes soient des logiciels malveillants que les utilisateurs installent sur leurs appareils. Les utilisateurs en font l'installation en cliquant sur le fichier pour aller voir ce fichier.

- **Rançongiciel (Ransomware)** : C’est une arnaque en ligne qui permet à un pirate informatique de verrouiller à distance l’ordinateur d’une personne et d’exiger un montant d’argent (une rançon) en échange d’un code pour déverrouiller l’ordinateur. Les transactions sont souvent faites en Bitcoins.

- **Fichier HEX :** C'est un format de fichier qu'on peut télécharger et qui est utilisé pour programmer un microcontrôleur (comme le micro:bit) ou d'autres composants programmables.

- **Hameçonnage (phishing)** : C'est une tactique employée par les pirates informatiques afin de nous piéger.

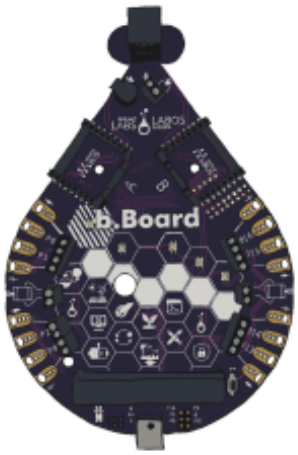
Avant le début de l'activité

Assurez-vous d'avoir en main le matériel et les outils nécessaires avant l'arrivée des élèves. Décider du meilleur mode de distribution du matériel. N'hésitez pas à demander à vos élèves de donner un coup de main. Pourquoi ne pas nommer un ou deux élèves responsables de préparer ce matériel avant la présentation de l'activité ? Nous vous suggérons des équipes de 4 ou 5 élèves pour cette activité.

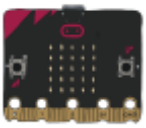
Matériel requis provenant de la trousse

La trousse contient plusieurs types de matériel qui sera utilisé tout au long de nos activités. Il n'est pas nécessaire de tout mettre à la disposition des élèves. Cela demeure à votre discrétion. Certains enseignants préfèreront mettre à la disposition des élèves seulement le matériel requis et d'autres pourront considérer l'accès total à la trousse par les élèves. Pour l'activité 2, vous aurez besoin du matériel suivant :

- 1 micro:bit par équipe ;
- 1 b.Board par équipe ;
- 1 Servo moteur ;
- 2 fils USB par équipe ;
- 2 bloc-piles (ces piles rechargeables vous permettront d'alimenter le micro:bit);2 fils USB par équipe ;
- 1 ordinateur avec accès à Internet par équipe.



b.Board



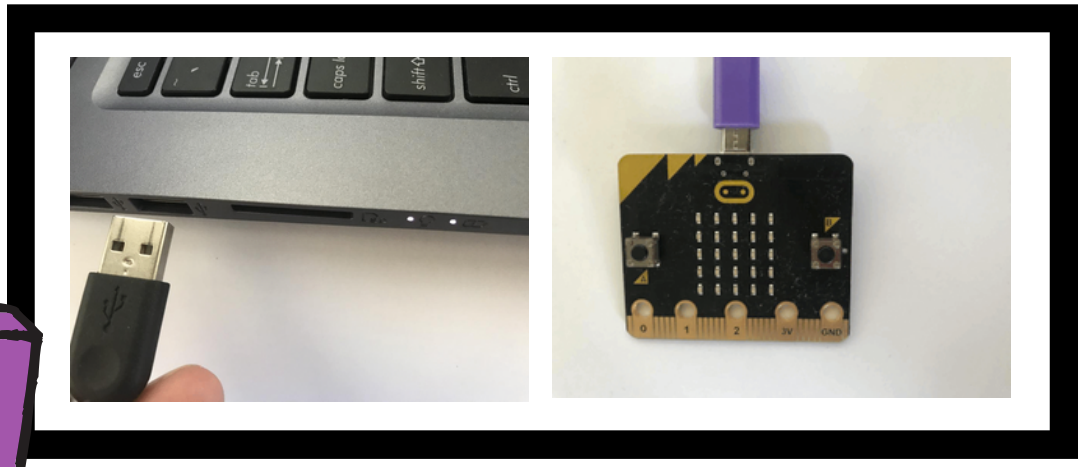
micro:bit
(V1 or V2)

Servo moteur

Partie 1 - Activité de programmation d'un micro:bit : Faire tourner un servo moteur

Le micro:bit est un microcontrôleur simple et vous aurez la chance de faire des activités de codage qui vous permettront de mieux comprendre comment se protéger et du fonctionnement du monde de la cybersécurité. Nous vous accompagnerons avec ceci et vous pourrez aussi donner du temps aux élèves pour explorer et essayer de créer leurs propres programmes.

Étapes à suivre pour brancher le micro:bit et le b.Board au portable

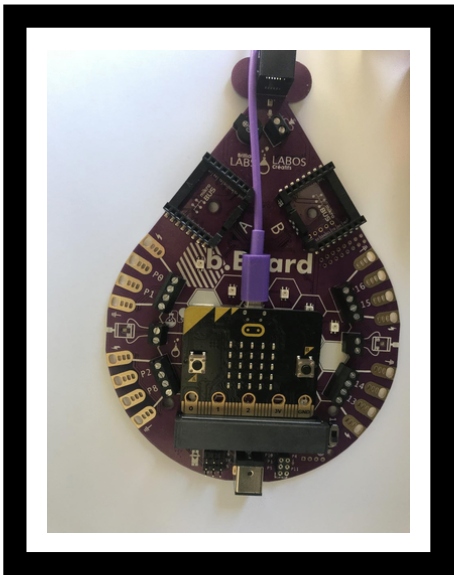


1

Brancher le fil USB à l'ordinateur (pas un iPad) et à l'autre extrémité du fil dans le micro:bit

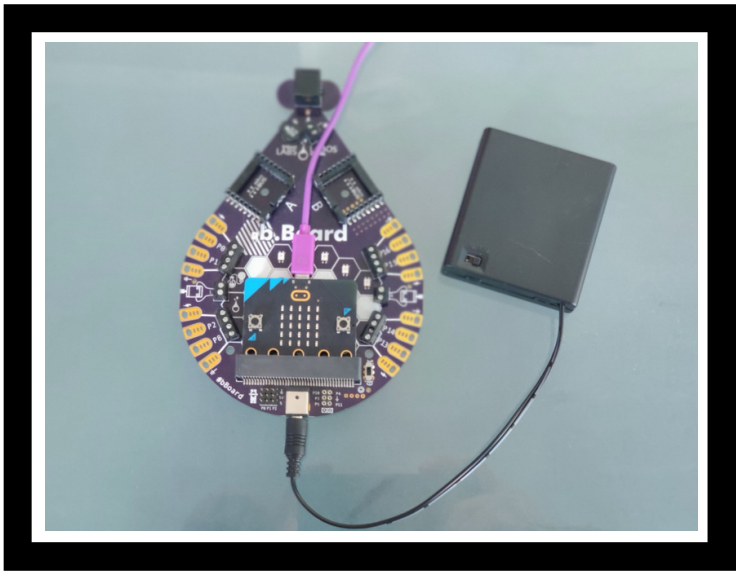
2

Insérer le micro:bit au B.board et assurez-vous que l'écran du micro:bit soit visible et les boutons A et B accessible.



Étapes à suivre pour brancher le micro:bit et le b.Board au portable

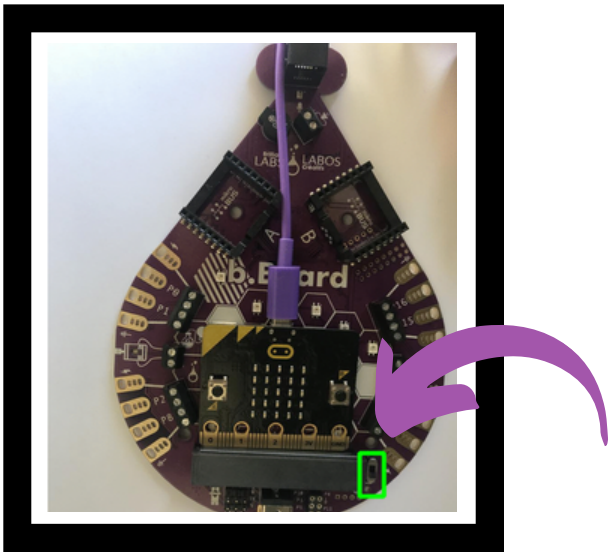
3



Assurez-vous que le b.Board soit branché à l'alimentation. Votre pile pourrait paraître différente de celle dans l'image.

4

Avec les connections complèter assurez-vous d'allumer l'interrupteur d'alimentation du b.Board.

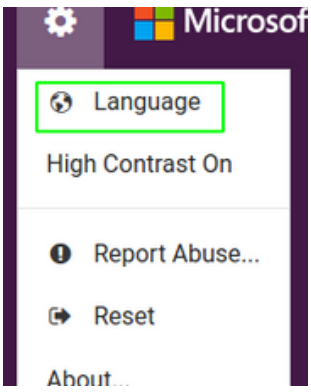


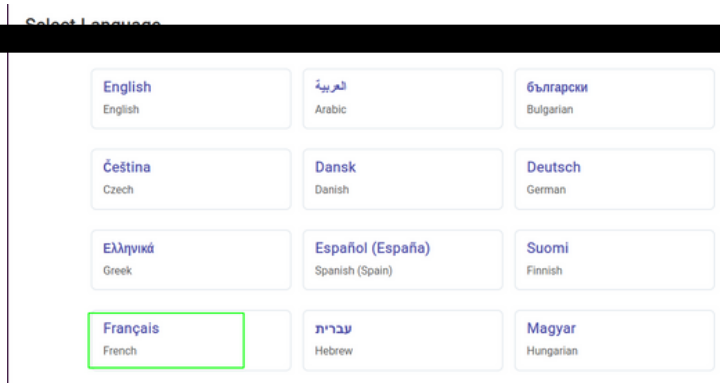
Étapes à suivre pour changer la langue de travail à Français

Il est possible que votre langue d'affichage soit déjà le français. Si c'est le cas, vous pouvez passer à la page suivante.

1

Veuillez vous rendre à l'adresse https://code.brilliantlabs.ca





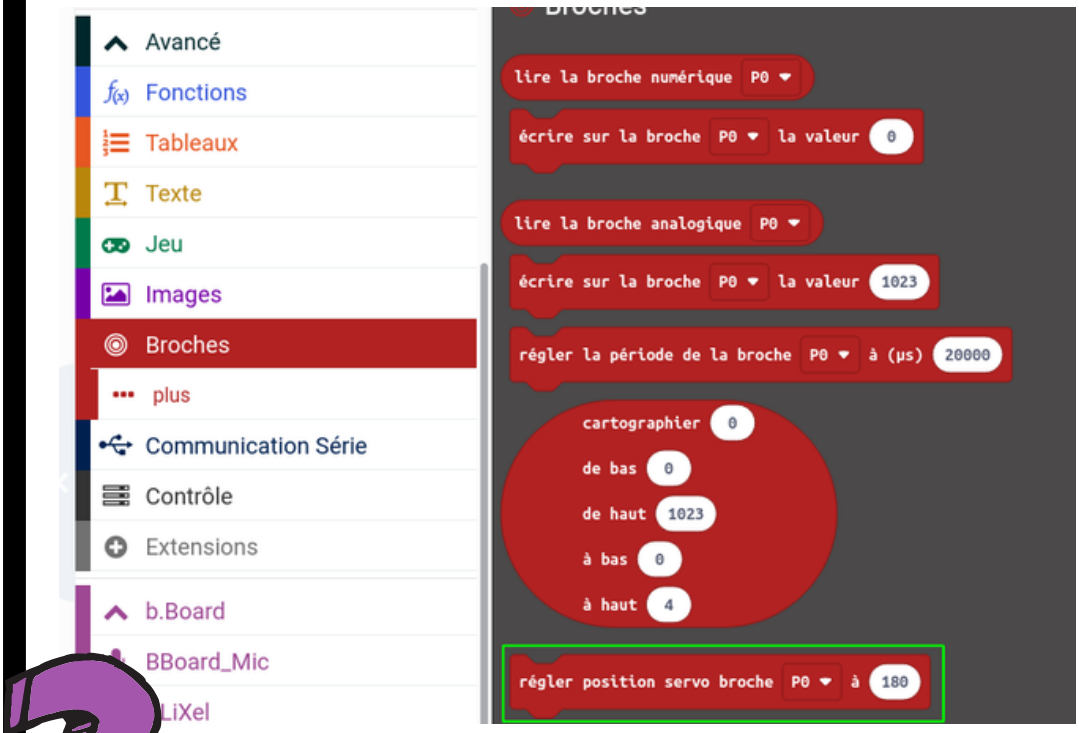
2

Ajuster la langue d'affichage à Français.

Étapes à suivre pour réaliser l'activité 3

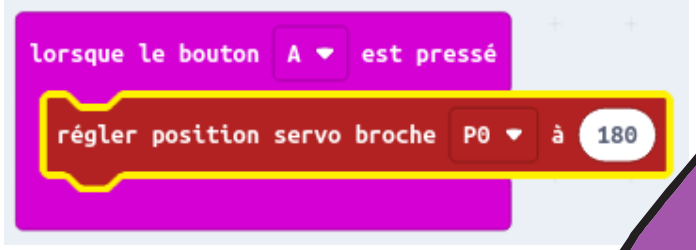
Donner un nom à votre activité en cliquant sur Nouveau Projet (ex : Activité 3)

Dans la section **Entrée**, apportez le bloc **lorsque le bouton A est pressé** sur le plan de travail.



3

Dans la section **Avancé**, et sous **Broches, apporter le bloc régler position servo broche P0 à 180** dans le bloc **lorsque le bouton A est pressé**.



4

Dans la section **Entrées**, apportez un deuxième bloc **lorsque le bouton A est pressé** sur le plan de travail. Changez A pour B.

Puis, dans la section **Avancé**, et sous **Broches**, apporter le bloc **régler position servo broche P0 à 180** dans le bloc l**orsque le bouton B est pressé**. Changez la valeur à 0.

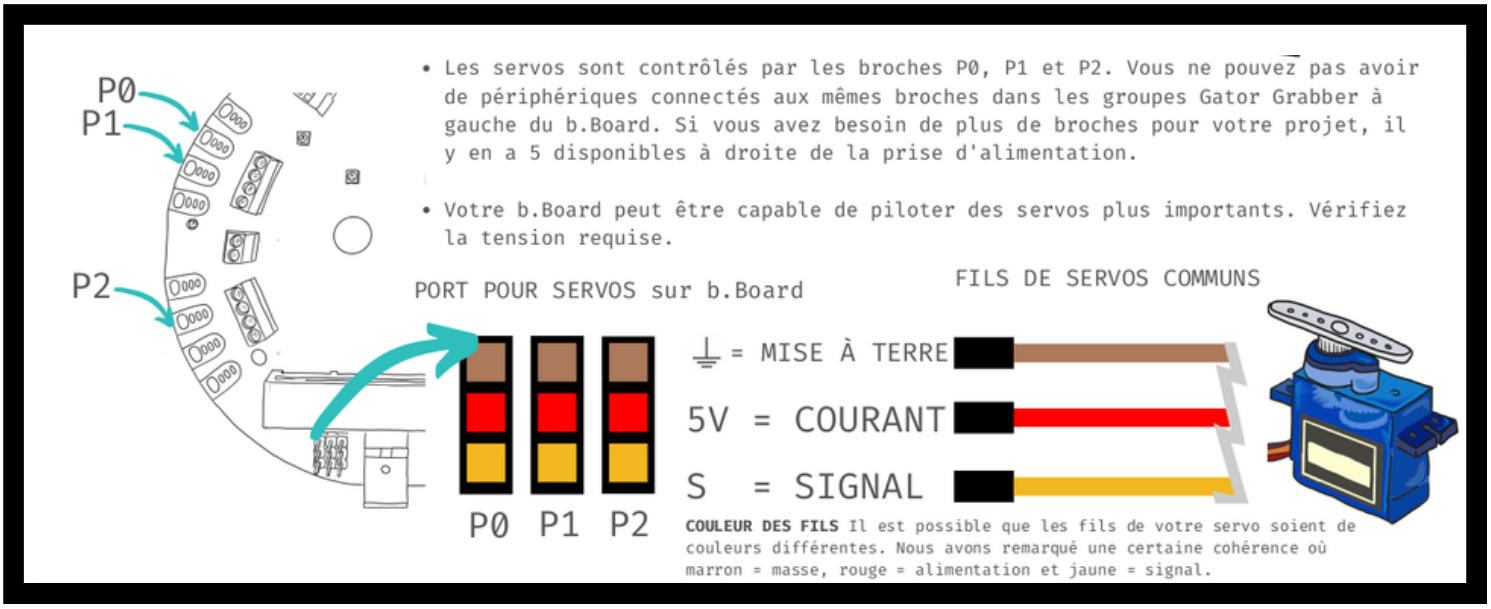
Explication du code

Le code que nous avons élaboré permet d'offrir 2 possibilités. Premièrement, lorsque nous allons appuyer sur le bouton A, le servo moteur tournera à 180 degrés.

En deuxième lieu, lorsque nous allons appuyer sur le bouton B, le servo moteur tournera dans le sens opposé.

Branchement du servo moteur

Pour visualiser le résultat de ce code, vous devrez brancher votre servo moteur au b.Board. La figure suivante démontre l'endroit où brancher votre servo moteur.



Étapes à suivre pour télécharger l'activité 3 dans le micro:bit

- Veuillez vous assurer que votre micro:bit est bel et bien branché à votre portable. Veuillez consulter la page 4 au besoin.
- Cliquez sur Télécharger et sauvegarder le fichier .hex dans le microbit.
- Appuyez sur le Bouton A et par la suite appuyez sur le Bouton B.

Un peu plus loin

Télécharger le fichier HEX

Fin de la partie 1

Partie 2 - Apprentissage en cybersécurité
Les logiciels malveillants

Laisser les élèves lire l'article ci-dessous et prendre le temps pour avoir une discussion en grand groupe. Vous pouvez projeter l'article sur un grand écran ou laisser les élèves découvrir l'article à partir de leur ordinateur.

Lien et source de l'article :
https://ici.radio-canada.ca/nouvelle/1766260/maliciel-dangereux-emotet-botnet-logiciel-cybersecurite

Questions à poser et discussion possible avec les élèves suite à la lecture de l'article

- Que retenez-vous à la lecture de cet article ?
- Pourquoi est-il important de savoir comment se protéger ?
- Utilisez-vous souvent les courriels ? Quels sont les avantages et les inconvénients ?
- Avez-vous déjà vécu une mauvaise expérience avec les logiciels malveillants ?
- Quels seraient des conseils à donner à vos amis ou aux membres de votre famille pour mieux se protéger avec les logiciels malveillants ?

Suggestions d'activités complémentaires possibles à faire en classe

- Écrire une lettre à un adulte pour expliquer l'importance des maliciels.
- Faire un dépliant sur l'importance des maliciels.
- Faire une affiche sur les trucs à utiliser pour se protéger des maliciels.
- Faire une vidéo pour expliquer les maliciels et comment se protéger.
- Faire un balado sur l'importance de se protéger contre les maliciels.

Suggestion de liens pour en savoir un peu plus et pour aller plus loin avec cette activité

Veuillez prendre note que les liens ci-dessous proviennent d'une tierce partie, Labos Créatifs n'est donc pas responsable de son contenu ou de liens suggérés publiés par ceux-ci. Nous vous suggérons fortement de prendre le temps d'aller visionner chacun de ces liens avant de les utiliser et de vous assurer qu'ils sont conformes à vos valeurs et à ce que vous utilisez normalement en classe avec vos élèves.

- Article, Radio-Canada : Cyberattaques aux États-Unies : un "risque grave", selon le gouvernement
- Vidéo YouTube : Maliciels et rançongiciels
- Vidéo YouTube : Hameçonnage : Ne mordez pas!
- Vidéo YouTube : L'hameçonnage
- Site Web du gouvernement du Canada: Qu'est-ce qu'un maliciel et comment vous en protéger?
- Infographie : Les outils de malveillance
- Page Web, Cybersécurité: base de données de ressources
- Page Web : Glossaire complet du Centre canadien pour la cybersécurité

Questions d'objectivation pour terminer l'activité

Vous pouvez aussi créer d'autres question si vous le jugez nécessaire.

- Qu'avons-nous appris avec cette activité ?
- Pourquoi est-ce important ?
- Allez-vous mettre certaines choses que vous avez apprises ?
- Comment est-ce que nous pouvons aider à diminuer l'impact de la malveillance en cybersécurité comme citoyen du 21e siècle ?
- Autres questions formulées par l'enseignant(e)...

Fin de l'activité 3