Thématique 3 : Sois Cyber secret

Un secret, c'est sacré

Mesurer l'importance de la confidentialité et de la sécurité

Aperçu de la thématique

Activité 1 : **Créer un mot de passe sécurisé**
Activité 2 : **Paramètres et sécurité**
Activité 3 : **La course aux mots de passe**
Activité 4 : **Mais ce n'était pas moi !**
Activité 5 : **Interland – La tour des trésors**
Conclusion : **Sois Cyber Secret**

Thèmes

Les problèmes de confidentialité et de sécurité en ligne n'ont pas toujours de solution évidente. Pour protéger vos informations personnelles et confidentielles, autrement dit tout ce qui *vous* caractérise, vous devez vous poser les bonnes questions et trouver vos propres réponses de manière réfléchie.

Objectifs des élèves

- ✓ **Découvrir** en quoi la confidentialité est importante et liée à la sécurité en ligne.
- ✓ **S'exercer** à créer des mots de passe sécurisés.
- ✓ **Passer en revue** les outils et les paramètres de protection contre les pirates informatiques et les autres menaces.

Un secret, c'est sacré
Vocabulaire

Chiffrement : processus de conversion d'informations ou de données en code pour les rendre illisibles et inaccessibles.

Complexité (d'un mot de passe) : fait de créer un mot de passe sécurisé. Par exemple, un mot de passe est complexe lorsqu'il mélange des chiffres, des caractères spéciaux (tels que "$" ou "&"), ainsi que des minuscules et des majuscules.

Confidentialité : fait de protéger les informations personnelles des utilisateurs (appelées également "informations sensibles").

Mot de passe ou code secret : combinaison secrète pour accéder à quelque chose. Elle peut prendre différentes formes : par exemple, vous devrez saisir un code à quatre chiffres pour verrouiller votre téléphone et un mot de passe plus complexe pour votre compte de messagerie. En général, vous devez faire en sorte que ce mot de passe soit long et complexe, tout en étant facile à retenir.

Pirate informatique (ou "hacker") : personne qui, à l'aide d'un ordinateur, cherche à accéder sans autorisation aux données et aux appareils d'autres entreprises, organisations ou utilisateurs.

Sécurité : fait de protéger les appareils des utilisateurs et les logiciels qui y sont installés.

Validation en deux étapes (appelée également "authentification à deux facteurs" ou "authentification en deux étapes") : processus de sécurité où la connexion à un service nécessite deux étapes ou "facteurs" distincts, comme un mot de passe et un code à usage unique. Par exemple, vous saisissez d'abord votre mot de passe, puis un code qui vous est envoyé par SMS sur votre téléphone ou provenant d'une application.

Virus informatique : les virus sont des programmes malveillants dont l'objectif principal est de perturber le bon fonctionnement d'un appareil, généralement un ordinateur. Ils servent parfois à voler des données ou des informations sur un appareil ou un réseau.

Un secret, c'est sacré (activité 1)

Créer un mot de passe sécurisé

Les élèves découvrent comment créer un mot de passe sécurisé et le garder confidentiel.

Objectifs des élèves

- ✓ **Mesurer** l'importance de ne jamais communiquer ses mots de passe, sauf à ses parents ou à son tuteur.
- ✓ **Comprendre** l'importance du verrouillage de l'écran pour protéger son appareil.
- ✓ **Apprendre** à créer des mots de passe difficiles à deviner, mais faciles à retenir.
- ✓ **Choisir** le bon système de sécurité pour se connecter.

Discussion

Mieux vaut prévenir que guérir

Les technologies numériques nous permettent de communiquer plus facilement avec nos amis, nos proches, nos camarades de classe et les enseignants. Nous pouvons entrer en contact avec eux de multiples façons : par e-mail, par SMS, par messagerie instantanée, ainsi qu'avec des mots, des photos et des vidéos, depuis un téléphone, une tablette ou un ordinateur portable.

Cependant, ces mêmes technologies permettent également aux pirates informatiques et aux fraudeurs de voler plus facilement nos informations et de les utiliser pour endommager nos appareils, altérer nos relations et entacher notre réputation.

Pour nous protéger et protéger également nos informations ainsi que nos appareils, il faut prendre quelques mesures simples : par exemple, verrouiller l'écran de notre téléphone, faire attention aux informations personnelles accessibles sur des appareils déverrouillés (qui peuvent être perdus ou volés) et, surtout, créer des mots de passe sécurisés.

- Qui sait quels sont les deux mots de passe les plus courants ? (Réponse : "1 2 3 4 5 6" et "motdepasse")
- Voyons ensemble d'autres mauvais mots de passe et pourquoi leur niveau de sécurité n'est précisément pas suffisant. (Exemples : votre nom complet, votre numéro de téléphone, le mot "chocolat")

Qui trouve que ce sont de bons mots de passe ? ;)

Activité

Voici une suggestion pour créer un mot de passe sécurisé :

- Pensez à une phrase facile à retenir (par exemple, les paroles de votre chanson préférée, le titre d'un livre que vous adorez, une petite phrase dans un film, etc.).
- Choisissez la première lettre ou les deux premières de chaque mot de cette phrase.
- Remplacez certaines lettres par des symboles ou des chiffres.

• Mettez certaines lettres en majuscule et d'autres en minuscule.
• Exercez-vous avec le jeu des mots de passe ci-dessous :

1. Créer des mots de passe
Formez deux équipes. Chaque équipe a 60 secondes pour créer un mot de passe.

2. Comparer les mots de passe
Les deux équipes écrivent en même temps leur mot de passe au tableau.

3. Voter
Tout le monde vote pour le mot de passe qui lui semble le plus sécurisé. Ensuite, nous allons en discuter.

Consignes pour créer un mot de passe sécurisé

Voici quelques conseils pour créer un mot de passe permettant de protéger vos informations.

Un mot de passe sécurisé est une combinaison de lettres, de chiffres et de symboles. Il peut être tiré d'une phrase facile à retenir, mais difficile à deviner constituée des premières lettres de votre chanson préférée ou de celles de plusieurs mots d'une phrase décrivant une action que vous avez accomplie. Par exemple, la phrase "En 2013, j'étais en classe de 3e primaire à l'école primaire du centre" peut servir à former le mot de passe "E2013jEcD3PaLpDc$".

Un mot de passe peu sécurisé est créé à partir d'informations personnelles basiques, non altérées - par exemple le nom de votre animal de compagnie. Il est donc facile à déchiffrer et risque d'être deviné par quelqu'un de votre entourage ou par un logiciel malveillant.

A FAIRE

- Utilisez un mot de passe différent pour chacun de vos comptes.
- Utilisez un mot de passe d'au moins huit caractères. Plus il est long, mieux c'est (à condition de vous en souvenir).
- Utilisez une combinaison de lettres (majuscules et minuscules), de chiffres et de symboles.
- Faites en sorte que vos mots de passe soient mémorisables pour que vous n'ayez pas besoin de les écrire quelque part (ce qui peut présenter un risque).
- Changez immédiatement de mot de passe si vous apprenez ou pensez qu'une personne (autre qu'un adulte de confiance) le connaît.
- Utilisez toujours un verrouillage d'écran sécurisé sur vos appareils. Paramétrez vos appareils de sorte qu'ils se verrouillent automatiquement s'ils se retrouvent entre de mauvaises mains.
- Créer un mot de passe unique et très long pour son adresse email. En effet celle-ci donne accès à de nombreux profils et applications et doit donc être particulièrement protégée.
- Pensez à utiliser un gestionnaire de mots de passe, tel que celui proposé dans votre navigateur, pour mémoriser vos mots de passe. De cette façon, vous pouvez utiliser un mot de passe unique pour chacun de vos comptes, sans avoir à les mémoriser tous.

A NE PAS FAIRE

- Ne créez pas votre mot de passe à partir d'informations personnelles (nom, adresse postale, adresse e-mail, numéro de téléphone, numéro de sécurité sociale, nom de jeune fille de votre mère, date de naissance, etc.) ni de mots courants.
- N'utilisez pas un mot de passe facile à deviner, comme votre surnom, le nom de votre école, votre équipe de rugby préférée, une suite de chiffres telle que 123456, etc. Et surtout, n'utilisez jamais le mot "motdepasse" !
- Ne communiquez votre mot de passe à personne, hormis vos parents ou votre tuteur.
- Ne notez jamais votre mot de passe là où une personne peut le trouver.

Conclusion

Créer un mot de passe sécurisé, c'est non seulement amusant, mais aussi essentiel.

Un secret, c'est sacré (activité 2)

Paramètres et sécurité

Sur un appareil de l'école, l'enseignant montre aux élèves comment procéder pour personnaliser leurs paramètres de confidentialité.

Objectifs des élèves

- ✓ **Personnaliser** les paramètres de confidentialité des services en ligne utilisés.
- ✓ **Définir** quelles informations peuvent être partagées ou non sur les sites et les services.
- ✓ **Comprendre** en quoi consistent l'authentification à deux facteurs et la validation en deux étapes, et quand s'en servir.

Discussion

La confidentialité et la sécurité sont tout aussi importantes

La confidentialité et la sécurité en ligne vont de pair. La plupart des applications et des logiciels offrent des moyens de contrôler quelles informations nous partageons et comment.

Lorsque vous utilisez une application ou un site Web, recherchez l'option intitulée "Mon compte" ou "Paramètres", par exemple. Vous pourrez ainsi accéder aux paramètres de confidentialité et de sécurité pour configurer les actions suivantes :

- Définir quelles informations sont visibles sur votre profil.
- Choisir qui peut consulter vos posts, vos photos, vos vidéos ou tout autre contenu que vous partagez.

Sur de nombreux réseaux sociaux, si la personne créant son compte est mineure, les informations personnelles, photos, posts sont automatiquements cachés pour les personnes que l'on ne connaît pas. Ceci n'est pas le cas lorsque la personne qui crée le compte est majeure. Mentir sur son âge lors de la création d'un compte peut donc avoir un impact sur la protection de nos données.

En apprenant à vous servir de ces paramètres pour protéger votre vie privée et en veillant à les tenir à jour, vous contrôlerez plus facilement la confidentialité et la sécurité de vos informations. Gardez à l'esprit que vous devez toujours définir ces paramètres avec vos parents ou votre tuteur. Vous devez également revoir ces paramètres de temps en temps : lors de mise à jour du réseau, ou lors de votre majorité, ceux-ci peuvent êtres modifiés sans que vous ne vous en aperceviez.

Activité

Étudier les options

L'appareil de l'école est branché sur le rétroprojecteur. Accédons à la page des paramètres de cette application pour voir quelles sont les options disponibles. Dites-moi comment effectuer les opérations suivantes :

- Modifier votre mot de passe.
- Accéder à vos paramètres de partage, de localisation et autres pour déterminer lesquels vous conviennent le mieux.
- Recevoir des alertes si une personne tente de se connecter à votre

Ressources nécessaires :

Appareil de l'école connecté à un rétroprojecteur pour une démonstration en classe visant à montrer un exemple de compte jugé approprié (par exemple, un compte de site Web ou de messagerie temporaire)

compte depuis un appareil inconnu.
- Rendre accessible votre profil en ligne (y compris les photos et les vidéos) uniquement aux membres de la famille et aux amis de votre choix.
- Activer l'authentification à deux facteurs ou la validation en deux étapes.
- Configurer les informations de récupération si vous ne parvenez plus à accéder à votre compte.

Pour déterminer les paramètres de confidentialité et de sécurité qui vous conviennent, vous devez en parler à vos parents ou à votre tuteur. N'oubliez pas que le paramètre de sécurité le plus important est votre cerveau. C'est vous qui décidez quelles informations personnelles partager, quand et avec qui.

Conclusion

Le choix d'un mot de passe unique et sécurisé pour chacun de vos comptes est une première étape essentielle. À présent, vous devez mémoriser ces mots de passe et les garder pour vous.

Un secret, c'est sacré (activité 3)

La course aux mots de passe

Comprendre l'importance de bien choisir son mot de passe et se familiariser avec les bons réflexes liés à la création de celui-ci.

Objectifs des élèves

- ✓ **Travailler** en équipe.
- ✓ **Apprendre** les bonnes pratiques de création d'un mot de passe.
- ✓ **Comprendre** les caractéristiques qui rendent un mot de passe sécurisé.

Activité

Ressources nécessaires :

- feuilles et stylos
- tableau blanc (avec feutres)
- dés à 6 faces (1 dé/groupe de participants)

1. Bien protéger vos mots de passe
Faire un petit tour de table avec les participants pour leur demander sur quels types de plateformes ils sont inscrits (réseaux sociaux, jeux vidéo, comptes divers), quelle importance ils accordent à la sécurité de ces comptes et sur quels critères ils se basent pour créer leurs mots de passe.

2. Place au jeu !
On va pouvoir maintenant mettre en place le jeu. Diviser le nombre de participants en 2 groupes. Chaque équipe détermine son mot de passe (avec certaines restrictions : types de caractères, nombre de caractères etc.). Le mot de passe doit avoir une longueur de 6 caractères, une majuscule, une minuscule et minimum un chiffre. Le reste des contraintes sont choisies par l'enseignant.

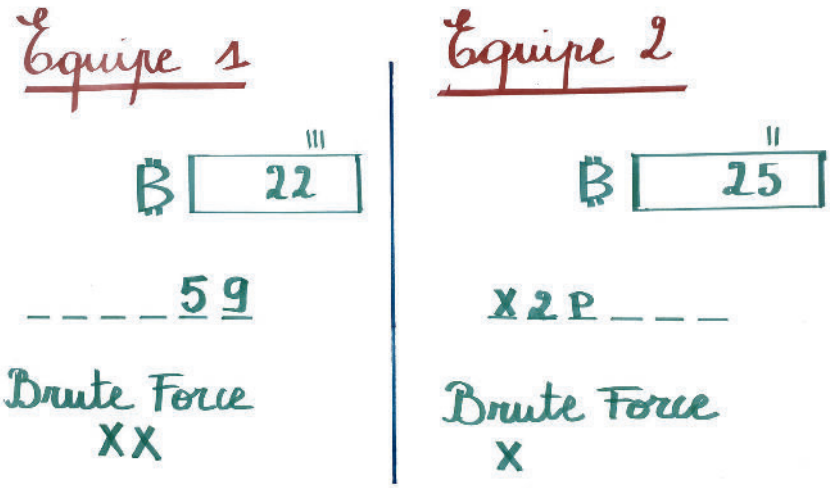
Contraintes possibles :

[A-Z] [a-z] [0-9] ! ?$

[A-Z] [a-z] [0-9] ! ?$.-_

[A-Z] [a-z] [0-9] ! ?$.-_@+

L'enseignant divise son tableau en 2 et détermine un montant égal de bitcoins pour les 2 équipes (par exemple, 30) qu'il écrit de chaque coté du tableau. Dans la même idée que le jeu du « pendu », il trace ensuite pour chaque équipe 6 tirets équivalant au nombre de caractères des mots de passe.



Chaque équipe, l'une après l'autre, va essayer de deviner une lettre du mot de passe de l'équipe adverse (toujours similaire au pendu), le nombre de tour est limité à 10 tours. A la fin des 10 tours, l'équipe qui a le plus de bitcoins restants sur son compte gagne, si une équipe réussit à deviner le mot de passe entier, il récupère la totalité de la somme restant sur le compte adverse.

L'équipe dont une lettre a été devinée se voit geler un bitcoin (représenté par un petit bâton au-dessus de la somme). Un bitcoin gelé est toujours compris dans le total du compte mais ne peut être utilisé pour faire une action.

Il existe 2 types d'actions que chaque équipe peut réaliser :

- Deviner une lettre au hasard (coûte 2 bitcoins à l'équipe qui effectue l'action).
- Utiliser le brute force (coûte 4 bitcoins à l'équipe qui effectue l'action).

Le Brute Force se matérialise par un lancer de dé par un membre de l'équipe qui effectue l'action. Le résultat affiché par le dé à six faces doit être supérieur à 3, s'il l'est alors l'équipe obtient directement la lettre qu'elle a essayé de deviner.

Infos supplémentaires : Bitcoin expliqué simplement
www.raspbian-france.fr/bitcoin-explique-a-ma-grand-mere/

3. Temps de partage :
Une fois le jeu fini, les équipes dévoileront leurs mots de passe (s'ils n'ont pas été devinés) et expliqueront les diverses étapes par lesquelles elles sont passées pour le créer. Et pourront donner leur avis sur la méthode empruntée par l'équipe adverse.

Pour pousser la réflexion, vous pouvez vous inspirer de cet article; « Le mot de passe est un mauvais système de sécurité. Mais il n'y en a pas de meilleur ».

http://www.slate.fr/story/90937/mots-de-passe-faut-il-en-finir

*Le Brute Force

Le Brute Force est l'une des méthodes qui peut être utilisée pour découvrir le mot de passe du compte d'une personne. Cette méthode consiste à lancer un logiciel dit de brute force, qui va essayer toutes les combinaisons possibles (numérique et/ou alphanumérique et/ou caractères spéciaux). Il est judicieux lors de l'utilisation d'un logiciel comme celui-ci de définir des pré-sets ce qui réduira le nombre d'essais (car très chronophage), l'on peut définir une limite de caractère ou prédéfinir certaines combinaisons. Il est possible par exemple de baser une "attaque" de brute force sur des informations relatives à la personne (noms/prénoms de proches, dates de naissance, adresse etc..) dans ce cas toutes les combinaisons possibles entre ces différentes informations seront essayées.

Pour comprendre que plus un mot de passe est long, plus celui-ci est efficace, ou bien encore comprendre l'intérêt d'utiliser des chiffres et caractères spéciaux, vous pouvez recommencer l'activité en durcissant ou simplifiant les contraintes (plus de caractères, interdire les caractères spéciaux, mettre des mots connus,...).

Conclusion

Bien choisir son mot de passe :
Vous allez maintenant pouvoir échanger avec les participants sur la méthodologie qu'ils ont choisie pour déterminer leurs mots de passe (et ce dont ils vous ont fait part lors de l'étape 1). Donnez leur des informations concernant la création d'un mot de passe : bien composer son mot de passe, comment stocker son mot de passe, quels sont les enjeux liés à la bonne protection de ses comptes et vous pouvez aussi parler rapidement du chiffrement des mots de passe ainsi que de l'authentification à 2 facteurs.

Ce contenu est proposé par Bibliothèques Sans Frontières.
Créé par Marion Piecuck.

Un secret, c'est sacré (activité 4)

Mais ce n'était pas moi !

Les élèves découvrent ce qui se passe lorsqu'ils communiquent leurs mots de passe et les conséquences que ces actions peuvent avoir.

Objectifs des élèves

- ✓ **Découvrir** qu'en donnant votre mot de passe à quelqu'un, cette personne peut prendre le contrôle de votre empreinte numérique.
- ✓ **Envisager** ce qui peut se produire quand quelqu'un se connecte en se faisant passer pour vous.
- ✓ **Comprendre** les conséquences des actions de quelqu'un d'autre sur votre empreinte numérique... et sur vous !

Discussion

Que se passe-t-il quand vous communiquez votre mot de passe ?
Pensez à un mot de passe que vous avez créé pour une application ou un appareil que vous utilisez. Ce mot de passe sert peut-être à déverrouiller votre téléphone ou à vous connecter à votre jeu ou application vidéo préféré(e). Avez-vous déjà donné votre mot de passe à quelqu'un ? Bon, soyons honnêtes : on l'a tous déjà fait. Mais s'il ne faut jamais communiquer votre mot de passe, c'est pour une bonne raison...

Vous avez ce que l'on appelle une empreinte numérique. L'empreinte numérique vous représente en ligne. C'est tout ce que vous laissez sur internet : des mentions « J'aime », des commentaires, votre pseudonyme, des photos, des messages, des enregistrements, etc. qui vous représentent et donnent aux autres une idée de ce que vous êtes réellement. Toutes ces actions ont des conséquences sur l'image que les autres ont de vous. Ils font des suppositions ou des hypothèses sur vous en fonction de l'empreinte numérique que vous laissez. C'est quelque chose de très important à savoir lorsque vous êtes en ligne.

Une autre chose très importante à savoir est que, lorsque vous communiquez votre mot de passe, vous donnez à quelqu'un d'autre le contrôle de votre empreinte numérique. Ainsi, vous l'autorisez à contribuer à créer votre image et à façonner ce que les autres pensent de vous. Étant donné qu'il s'agit de votre empreinte, tout le monde pense que c'est vous qui la créez. Donc si quelqu'un a votre mot de passe et fait quelque chose que vous n'aimez pas, les autres vont croire que c'est vous ! C'est la raison pour laquelle il est extrêmement important de ne pas communiquer vos mots de passe.

Exemple : Imaginons que vous donniez le mot de passe de votre compte sur un réseau social à un ami. En se connectant en votre nom, votre ami envoie un message à un camarade de classe comme : « Tu peux m'envoyer les réponses aux devoirs ? » Le jour suivant en classe, l'élève va voir le professeur et lui dit que vous avez essayé de tricher en lui demandant les réponses au devoir. Ensuite, il montre à votre professeur le message que votre ami a envoyé depuis votre compte. Qui selon vous

le professeur va-t-il croire ? Quelle sera la conséquence sur votre image ? Qu'est-ce qui pourrait encore se passer ?

Discutez avec la classe des conséquences éventuelles. Exemples : votre professeur appelle vos parents. Vous perdez des points à un exercice. Votre empreinte numérique montre que vous avez essayé de tricher à l'école. Vous vous battez avec votre ami qui a envoyé le message.

N'oubliez pas, votre empreinte numérique vous représente en ligne. Dès que vous donnez votre mot de passe à quelqu'un, vous lui donnez le contrôle de votre empreinte numérique, ce qui peut avoir des conséquences sur l'opinion que les autres ont de vous sur internet et dans la vie. Parlons de cette idée.

Activité

Ressources nécessaires :

- Fiche d'exercices : « Mais ce n'était pas moi ! » (une pour chaque groupe de deux).

1. Aider les élèves à se mettre par deux

2. Choisir un compte
Les élèves choisissent le type de compte pour lequel ils communiquent leur mot de passe et le notent en haut de la fiche d'exercices (compte d'un réseau social, compte d'un jeu en ligne, téléphone, tablette/ordinateur, service de streaming).

3. Choisir une action
Les groupes de deux remplissent la première case en indiquant une action qu'ils choisissent dans les propositions ci-dessous ou qu'ils inventent eux-mêmes. C'est une action effectuée par quelqu'un qui a reçu le mot de passe de leur compte. Ils peuvent dessiner ou écrire leurs idées ou faire leur choix parmi les actions possibles suivantes :

- Ajouter des mentions « J'aime » à tous les posts de la personne dont vous êtes secrètement amoureux.
- Acheter des vêtements pour un montant de 100 €.
- Envoyer un message comme « Tu trouves pas que Carmen est embêtante ? »
- Jouer à votre jeu préféré, mais en perdant des points.
- Partager une photo compromettante sur votre profil d'un réseau social.
- Lire tous vos messages et les envoyer à quelqu'un d'autre.
- Regarder des épisodes d'une série TV inappropriée.

4. Imaginer une conséquence
Dans la deuxième case, les élèves imaginent une conséquence possible à l'action qu'ils ont choisie ou créée.

5. Discussion
Demandez à quelques élèves d'expliquer au reste de la classe l'action et les conséquences qu'ils ont imaginées. Voici quelques questions que vous pourriez poser aux groupes une fois qu'ils ont expliqué leur exercice :

- Pourquoi avez-vous choisi (ou créé) cette action ?
- Comment avez-vous décidé de la conséquence ?
- Si vous connaissiez la conséquence, dans quelle mesure changeriez-vous votre action ?

6. Empreinte numérique
Dans la dernière case, les élèves écrivent une phrase sur l'impact de cette action et de ses conséquences sur leurs émotions, leur vie ou leur empreinte numérique, individuellement ou dans l'ensemble. Amenez les élèves à réfléchir sur l'incidence de cette action sur leur image en ligne et la manière dont les autres les considèrent. Demandez à des volontaires ou à des groupes de deux élèves de discuter de ce qu'ils ont dessiné ou écrit et de ce qu'ils pensent de l'histoire qu'ils ont créée.

Conclusion

Lorsque vous communiquez votre mot de passe, vous donnez à quelqu'un d'autre le contrôle de votre empreinte numérique, mais vous êtes toujours responsable de ce qu'il en fait. Si vous voulez rester maître de votre image en ligne, ne donnez jamais votre mot de passe à quelqu'un, si ce n'est à un parent ou à un autre adulte en qui vous avez totalement confiance. Et si vous voulez vraiment partager un mot de passe (par exemple un compte Netflix avec des amis), assurez-vous que ce mot de passe ne soit pas utilisé pour un autre de vos comptes.

Mais ce n'était pas moi !

J'ai donné le mot de passe de

- ☐ mon compte de réseau social
- ☐ ma tablette/ mon ordinateur
- ☐ mon compte de jeu en ligne
- ☐ mon service de streaming
- ☐ mon téléphone
- ☐ .....

.....

Action

Conséquence

Impact sur l'empreinte numérique

Un secret, c'est sacré (activité 5)

Interland : La tour des trésors

SOS ! La porte de la tour des trésors n'est pas fermée à clé et toutes les précieuses données des internautes sont sans protection comme les coordonnées et les messages privés. Déjouez le plan néfaste du pirate informatique en bâtissant une forteresse avec des mots de passe sécurisés qui protègent tous vos secrets une fois pour toutes.

Depuis votre ordinateur ou votre appareil mobile (une tablette, par exemple), ouvrez un navigateur Web et rendez-vous sur https://beinternetawesome.withgoogle.com/fr_be/interland/tower-of-treasure.

Discussion

Demandez aux élèves de jouer à "La tour des trésors" et de répondre aux questions ci-dessous pour discuter ensuite plus en détail des enseignements à tirer de ce jeu. Même si la plupart des élèves qui y jouent seuls en retirent plus de bénéfices, vous pouvez également former des groupes de deux. Cela peut être très instructif pour les jeunes élèves.

- Quels sont les critères à respecter pour créer un mot de passe sécurisé ?
- Dans la vraie vie, quand est-il important de créer des mots de passe sécurisés ? Comment vous a-t-on conseillé de procéder ?
- Qu'est-ce qu'un pirate informatique ? Décrivez son comportement et son influence sur le jeu.
- Ce jeu va-t-il changer votre façon de protéger vos informations ?
- Citez une chose que vous feriez différemment après avoir suivi ces thématiques et joué à ce jeu.
- Imaginez trois mots de passe qui répondent aux critères d'un mot de passe sécurisé.
- Citez des exemples d'informations sensibles à protéger.

Sois cyber secret

CRÉER UN MOT DE PASSE SÉCURISÉ, C'EST NON SEULEMENT AMUSANT MAIS ESSENTIEL !

Retrouve les mots manquants dans ces consignes. Pour t'aider, voici la liste des mots à replacer aux bons endroits dans le texte.

écran – sécurisé – symboles - mémorisables – chiffres - change – personnelles – différent – risque – confiance – lettres – huit

Consignes pour créer un mot de passe _____.

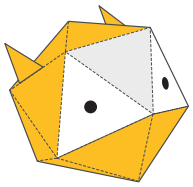
- Utilise un mot de passe _____ pour chacun de tes comptes.
- Utilise un mot de passe d'au moins _____ caractères.
- Utilise une combinaison de _____ (majuscules ou minuscules), _____ et _____ .
- Fais en sorte que tes mots de passe soient _____ pour que tu n'aies pas besoin de les écrire quelque part (ce qui peut présenter un _____).
- _____ immédiatement de mot de passe si tu apprends ou si tu penses qu'une personne, autre qu'un adulte de _____ le connait.
- Utilise toujours un verrouillage d'_____ sécurisé sur tes appareils. Paramètre-les de sorte qu'ils se verrouillent automatiquement s'ils se retrouvent entre de mauvaises mains.
- Ne crée pas ton mot de passe à partir d'informations _____ ni de mots courants.

Entoure les mots de passe qui sont les plus sécurisés :

1a7R9b$8reE
j'aimelespizzas
Qlbarbecue70&5555
1234Nathan
#eS47gKdR=@
Cookie

Réponses : sécurisé/ différent/ huit/ lettres/ chiffres/ symboles/ mémorisables/ risque/ change/ confiance/ écran/ personnelles. Mots de passe sécurisé : 1a7R9b$8reE / Qlbarbecue70&5555 / #eS47gKdR=@

Les Cyber Héros



Couper

Plier

Coller

Un secret, c'est sacré

- Prenez vos responsabilités afin de protéger les informations importantes.
- Choisissez un mot de passe unique et facile à mémoriser.
- Créez un mot de passe fort en associant des lettres, des chiffres et des symboles.

Sois cyber secret