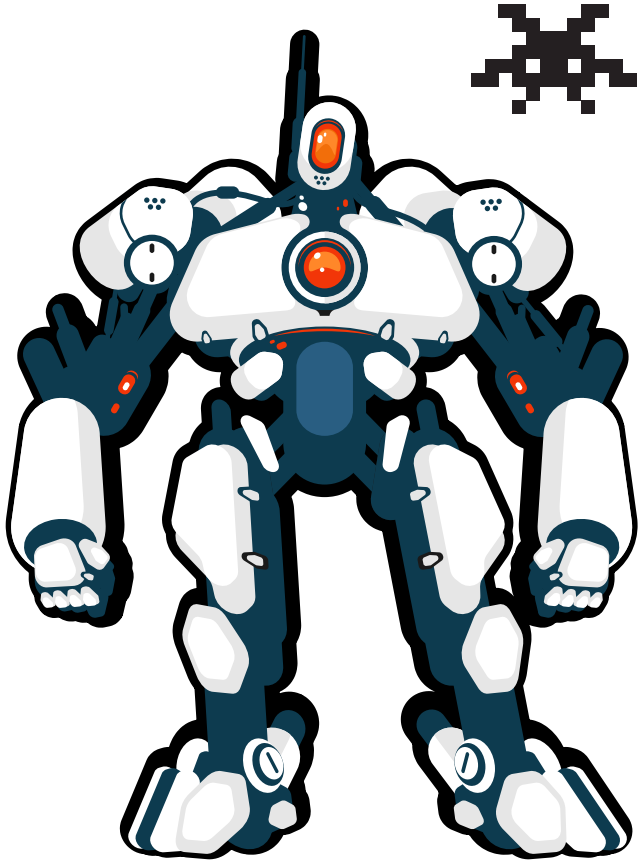
Agence Pensez cybersécurité

Cahier d'exercices pour enfants



Numero de catalogue : D96-84/2022F-PDF | ISBN : 978-0-660-42556-6

Centre de la sécurité des télécommunications | Communications Security Establishment

PENSEZCYBERSECURITE.CA

Canada

Jeu 1 : Les phrases de passe – un code indéchiffrable

Voici ta première mission!

Bonjour, et bienvenue à toi, Cyberagent! Je suis Cybot, ton partenaire. Ensemble, nous allons combattre le cybercriminel, Viro. Il attaque les gens sur Internet et les vole. Nous devons absolument l'arrêter!

Prêt(e) à commencer? Super! La première étape pour vaincre Viro sera de te créer une **phrase de passe**.

Réponds au jeu-questionnaire suivant pour tester tes connaissances de cyberagent en matière de mots de passe et de **phrases de passe**.

Durant ta mission, si tu vois un mot que tu ne comprends ou ne connais pas, tu peux en chercher la définition dans le glossaire qui se trouve à la page 21 de ce cahier!
Bonne chance, Cyberagent!

Formation de cyberagent – phrases de passe

Instructions :

Réponds aux questions suivantes en encerclant la bonne réponse. Tu trouveras la solution à toutes les questions du jeu-questionnaire au verso du cahier!

Question 1 : Quand peut-on partager un mot de passe?

A Jamais.

B Seulement avec nos meilleur(e)s ami(e)s.

C Lorsqu'une autre personne en a besoin.

Indice : Les mots de passe protègent **tous** les renseignements qui figurent sur ton compte!
Indice : Les mots de passe sont **très** personnels!

Question 2 : Vrai ou faux? On peut utiliser en toute sécurité le même mot de passe pour plusieurs comptes.

A Vrai.

B Faux.

Indice : Si un cybercriminel vole ton mot de passe, il peut accéder à **tous tes comptes** pour lesquels tu utilises ce mot de passe.

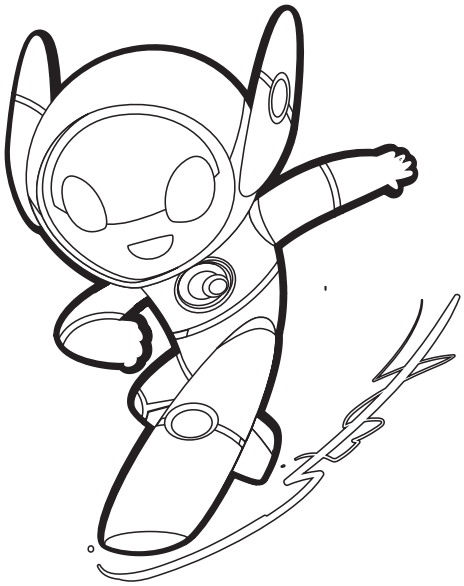
Question 3 : Quel type de mot de passe est le plus robuste?

A Une phrase de passe qui contient quatre mots aléatoires ou plus.

B Un mot de passe qui est aussi court que possible.

C Un mot de passe qui contient le nom de ton animal de compagnie.

Indice : Un mot de passe ne doit jamais comprendre des renseignements personnels.
Indice : Les mots de passe les plus longs sont les plus robustes!



Jeu 1 : Un code indéchiffrable

Beau travail, Cyberagent!

Afin de poursuivre notre mission, nous devrons créer une phrase de passe robuste et top secrète pour protéger nos fichiers et nos comptes de cyberagent contre Viro, et contre d'autres cybercriminels. Maintenant que tu sais ce que sont les mots de passe et les phrases de passe, créons ensemble ta propre phrase de passe!

Comment jouer

- → Réponds à **quatre** des questions et énoncés ci-dessous.
- → Essaye de trouver des **réponses formées d'un seul mot** comportant **un minimum de 4 lettres**.
- → Dans **les quatre cases qui suivent**, inscris tes réponses pour obtenir ta **phrase de passe** top secrète!
- → Tu peux utiliser ta phrase de passe pour l'un de tes comptes ou de tes appareils. N'oublie pas qu'il est important d'utiliser une phrase de passe unique pour chaque compte!

Réponds à quatre des questions ci-dessous pour créer ta phrase de passe top secrète!

Quel est le légume que tu aimes le moins? _____

Si tu avais 100 $ à dépenser, qu'achèterais-tu? _____

Nomme une chose de couleur bleue que tu vois en ce moment même. _____

Qu'as-tu mangé pour dîner hier? _____

Quel est le jour de la semaine aujourd'hui? _____

Choisis au hasard un mot qui commence par la lettre L. _____

Nomme un objet qui se trouve dans la cuisine chez toi. _____

Ta phrase de passe top secrète est :

Beau travail, Cyberagent!

Maintenant que tu as créé ta phrase de passe top secrète, tu peux commencer ta prochaine mission.

Jeu 2 : Les outils – Les outils spéciaux

Excellent travail : tu as créé une phrase de passe super robuste et top secrète!

Maintenant, amusons-nous avec nos outils! Nous devons choisir les outils qui nous permettront de vaincre Viro et son équipe de cybercriminels.

De quoi aurons-nous besoin? D'abord, il nous faudra un **logiciel antivirus** pour empêcher que des fichiers malveillants, appelés **maliciels**, corrompent tes fichiers. Nous devrons aussi avoir un **disque dur** ou suffisamment d'espace dans le **nuage** pour pouvoir faire des sauvegardes de tes fichiers importants. Enfin, n'oublie surtout pas cette autre arme importante : l'**authentification multifactorielle** avec empreinte digitale ou code de sécurité.

Nous avons d'excellents outils à notre disposition pour combattre Viro. Faisons la formation de cyberagent qui suit pour bien comprendre leur fonctionnement.

Formation de cyberagent – outils

Instructions :
Réponds aux questions suivantes en encerclant la bonne réponse. Tu trouveras la solution à toutes les questions du jeu-questionnaire au verso!

Question 1 : Comment sauvegarde-t-on un fichier?

A On sauvegarde le même fichier deux fois sur le même appareil.

B On sauvegarde une copie du fichier sur un autre appareil.

C On supprime le fichier.

Indice : Les sauvegardes protègent tes fichiers si quelque chose arrive avec ton appareil.
Indice : Il faut stocker tes sauvegardes dans un endroit sécuritaire.

Question 2 : Qu'est-ce que l'authentification multifactorielle?

A Un deuxième moyen de prouver que tu es bien la personne que tu prétends être (cela peut être un code de sécurité de type **NIP** ou une empreinte digitale).

B Deux mots très longs.

C Une énigme pour mystifier les cybercriminels.

Indice : L'authentification multifactorielle est utilisée pour te connecter et pour ouvrir une session, comme tu le fais pour certains jeux vidéo.
Indice : Le mot « authentification » signifie « confirmer qu'une chose est vraie ».

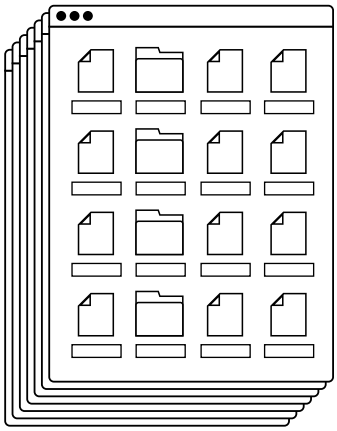
Question 3 : Quand dois-tu faire les mises à jour logicielles?

A Dès que je le peux.

B Lorsque mon téléphone est super lent.

C Lorsque le message de rappel ne disparaît pas de l'écran.

Indice : Les mises à jour logicielles protègent tes appareils.
Indice : Il est préférable de faire tes mises à jour **avant** qu'un incident ne se produise!



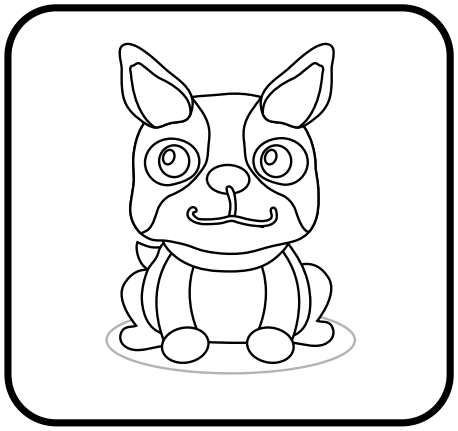
Jeu 2 : Les outils spéciaux

Beau travail, Cyberagent!

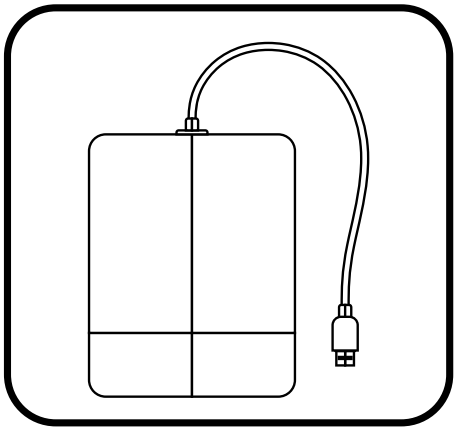
Maintenant que tu sais comment protéger tes outils, c'est l'heure d'assembler notre trousse d'outils pour accomplir la prochaine mission!

Comment jouer

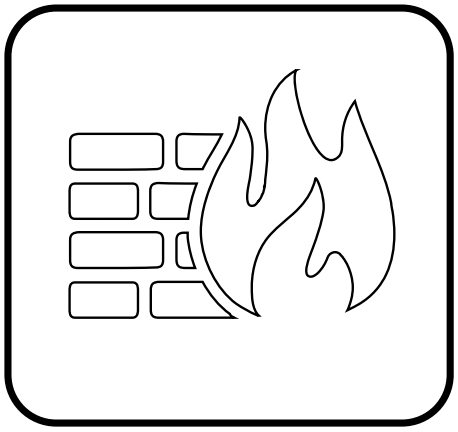
Assemble ta trousse d'outils pour la prochaine mission en coloriant seulement ceux dont nous avons besoin pour vaincre Viro. Ne colorie pas ceux dont nous n'avons pas besoin! Tu peux vérifier si tu as choisi les bons outils en consultant la page suivante!



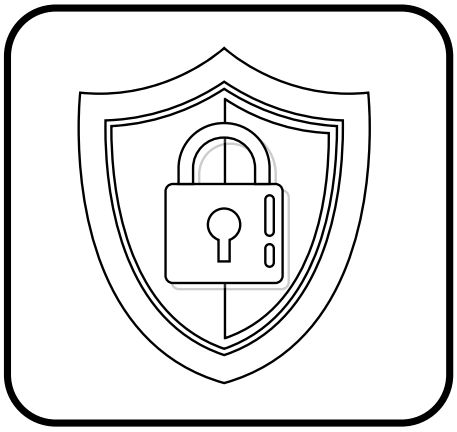
Chiot



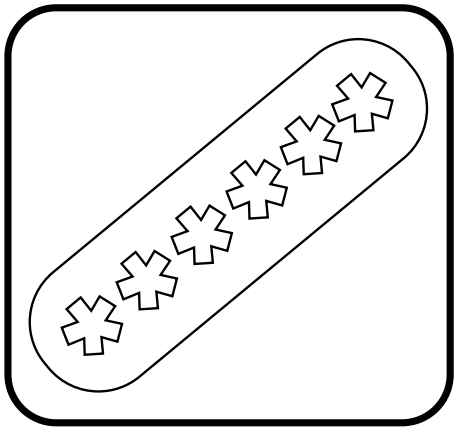
Disque dur



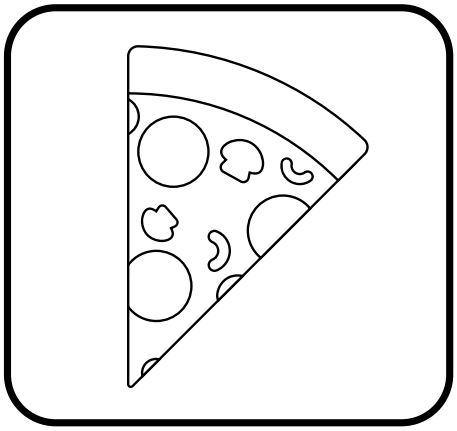
Pare-feu



Logiciel antivirus



Phrase de passe

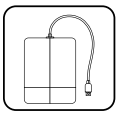


Pizza

Réponses au jeu des outils spéciaux

Logiciel antivirus : Bonne réponse, tu en auras besoin!

Le logiciel antivirus empêchera les fichiers malveillants et les virus d'infecter nos outils!

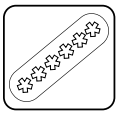


Disque dur : Bonne réponse, tu en auras besoin!

Un disque dur est idéal pour sauvegarder tous nos fichiers importants afin de ne jamais les perdre.

Chiot : Oups, tu n'auras pas besoin de ça!

Les bébés chiens sont d'adorables petites bêtes, mais ils ne sont pas très doués en cybersécurité!



Phrase de passe : Bonne réponse, tu en auras besoin!

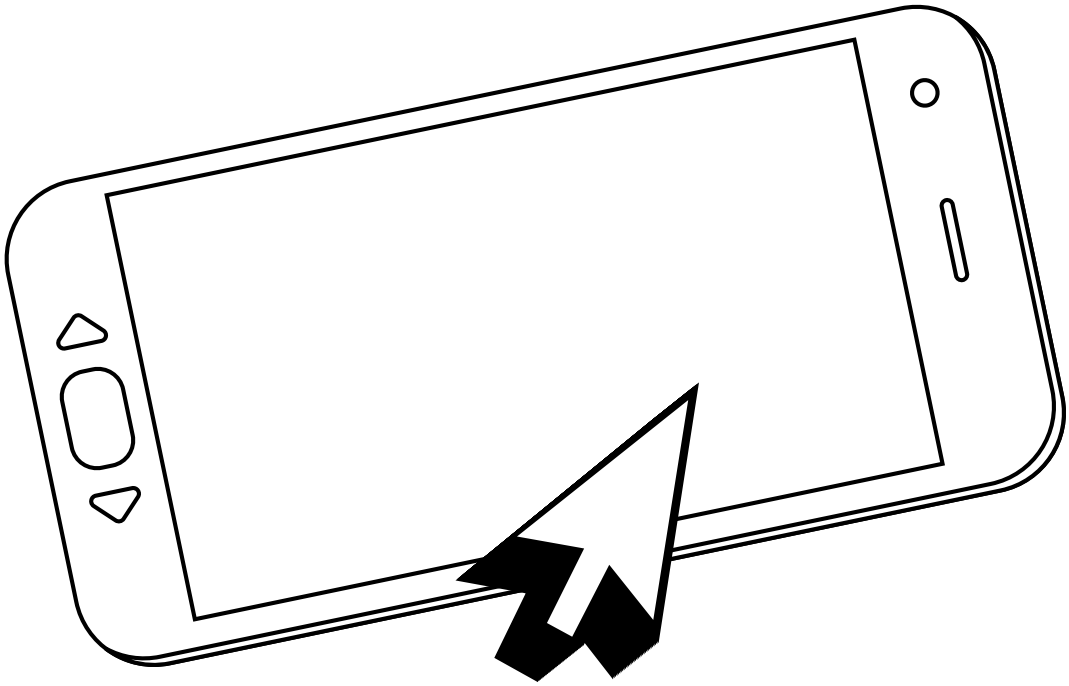
Une phrase de passe est comme un mot de passe, mais elle est plus longue et plus sûr!

Pare-feu : Bonne réponse, tu en auras besoin!

Les pare-feu sont conçus pour protéger nos appareils lorsqu'ils sont connectés à l'Internet!

Pizza : Oups, tu n'auras pas besoin de ça!

La pizza a certainement bon goût, mais elle ne nous aidera pas à vaincre Viro!



Jeu 3 : Wi-Fi/Réseaux – objectif routeur

Excellent travail!

Maintenant que nous avons notre trousse d'outils, il faut les protéger contre Viro. Peux-tu m'aider à configurer notre **routeur Wi-Fi**? C'est un petit appareil qui permet aux autres appareils, comme les tablettes électroniques et les téléphones, de se connecter à Internet. Révisons notre liste pour nous assurer que nous sommes bien protégés.

D'abord, il faut que le routeur soit placé loin d'une fenêtre. Il faut ensuite créer un mot de passe robuste pour le routeur en utilisant une phrase de passe! Plus tard, tu pourras demander à un adulte de confiance de t'aider à configurer ton routeur à la maison.

Prêt(e) à foncer? Travaillons ensemble pour sécuriser notre routeur.

Formation de cyberagent – routeur Wi-Fi

Instructions :
Réponds aux questions suivantes en encerclant la bonne réponse. Tu trouveras la solution à toutes les questions du jeu-questionnaire au verso du cahier!

Question 1 : Vrai ou faux? Mettre tes appareils à jour permet d'assurer la sécurité de ton réseau.

A Vrai.

B Faux.

Indice : Mettre à jour tes appareils peut aider à les protéger.

Question 2 : Chez toi, quel est l'endroit le plus sûr pour installer ton routeur?

A Juste en face de la porte d'entrée.

B Au centre de la maison.

C Caché avec tes jouets.

Indice : Un **routeur** est un petit appareil qui permet aux autres appareils, comme les tablettes électroniques et les téléphones, de se connecter à Internet.
Indice : Plus tes appareils sont situés près du routeur, plus ton réseau Wi-Fi sera puissant et rapide!
Indice : Les cybercriminels peuvent accéder à ton réseau Wi-Fi plus facilement s'ils sont plus près de ton routeur, par exemple, si ce dernier est devant une fenêtre.

Question 3 : La première fois que tu installeras un routeur, il possèdera un mot de passe par défaut. Pourquoi devrais-tu changer ce mot de passe?

A Parce que les cybercriminels peuvent accéder plus facilement à ton réseau Wi-Fi si tu ne changes pas ce mot de passe.

B Parce que plusieurs routeurs peuvent avoir le même mot de passe par défaut.

C A et B.

Indice : Tu ne devrais jamais garder un mot de passe qui t'a été donné!
Indice : Tu peux utiliser un **gestionnaire de mots de passe** pour te souvenir de tous tes mots de passe ou de tes phrases de passe plus longues.
Indice : Les cybercriminels savent bien déchiffrer les mots de passe.

Jeu 3 : Objectif routeur

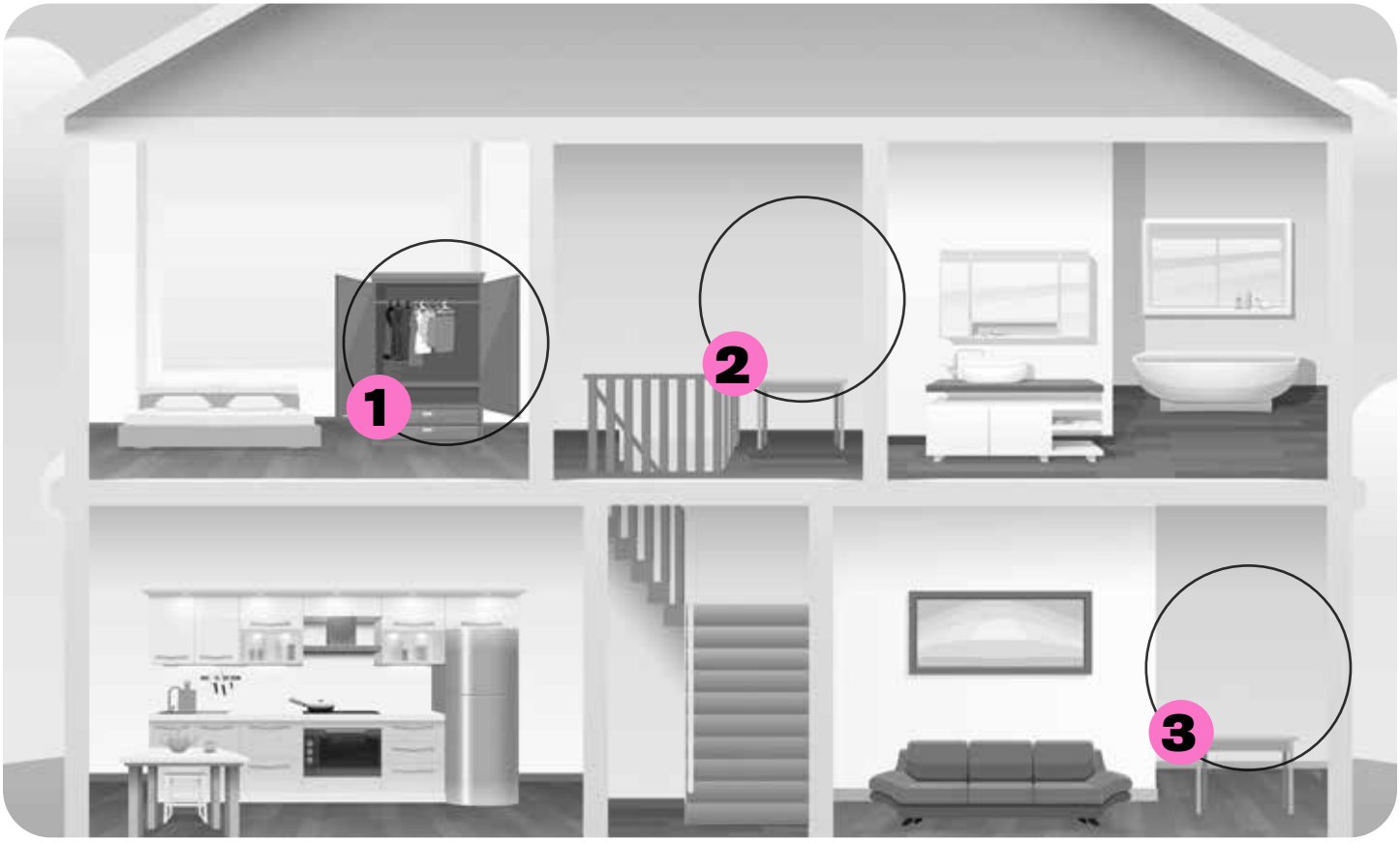
Excellent travail, Cyberagent! Maintenant que tu sais comment protéger ton réseau Wi-Fi, faisons de notre mieux pour empêcher Viro d'y accéder!

Nous venons d'apprendre que Viro prépare une cyberattaque contre nous. Sécurisons notre réseau Wi-Fi avant qu'il ne passe à l'action!

Comment jouer

→ Dans un des trois cercles vides dans l'image ci-dessous, dessine un routeur à l'endroit le plus sûr de la maison. Tu peux faire un dessin du routeur qui est chez toi (si tu ne sais pas où il se trouve, demande à un adulte) ou bien de celui qui se trouve dans le coin de cette page.

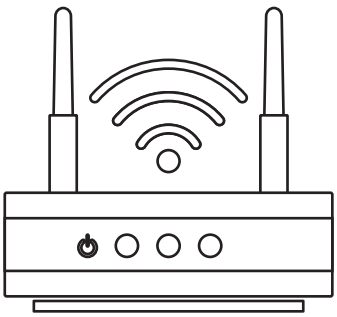
→ Une fois ton dessin terminé, tourne la page pour voir si tu as réussi à placer le routeur au bon endroit!



Emplacement 1 : Dans un placard

Emplacement 2 : Au centre de la maison

Emplacement 3 : Devant une fenêtre

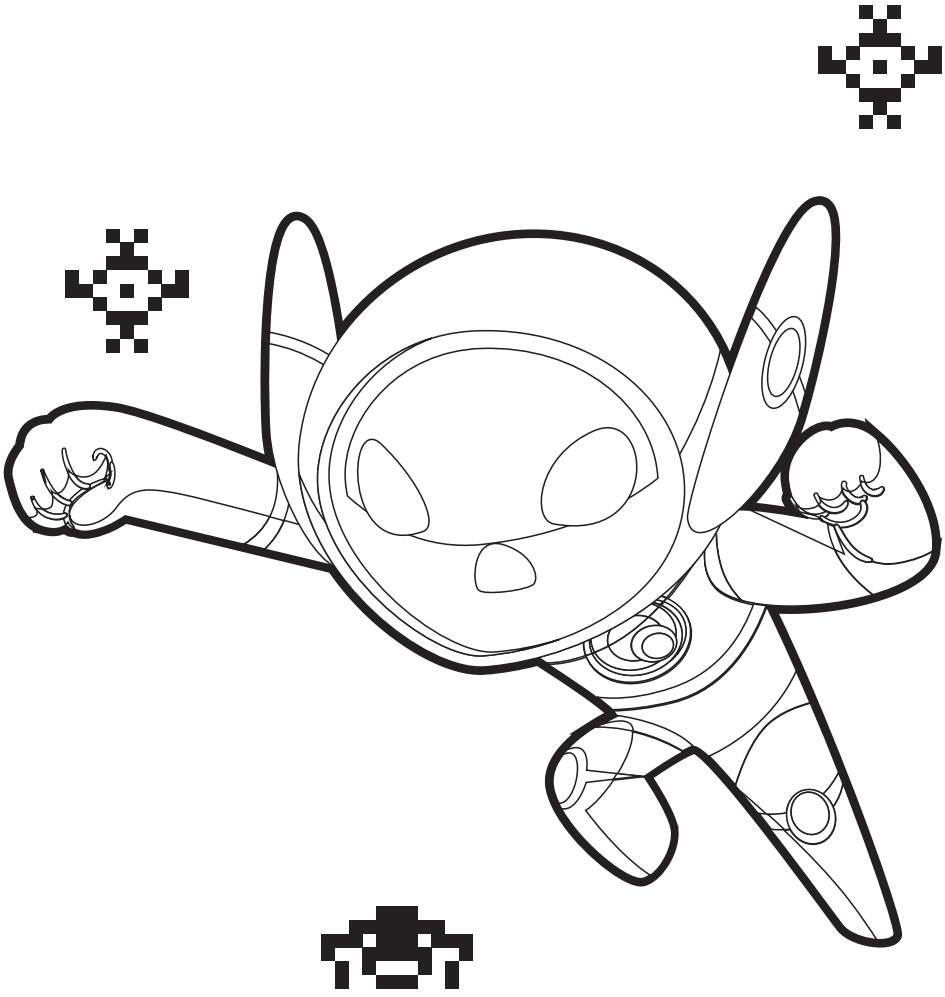


Réponses

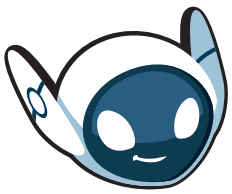
Emplacement 1 (Dans un placard) **:** Essaye encore! Si le routeur est rangé quelque part, par exemple dans un placard, il peut être difficile pour toi et ta famille de vous connecter au Wi-Fi!

Emplacement 2 (Au centre de la maison) **:** Bonne réponse! En installant le routeur au centre de la maison, il est plus facile pour toi et ta famille de vous y connecter, et plus difficile pour les cybercriminels d'y accéder!

Emplacement 3 (Devant une fenêtre) **:** Essaye encore! Plus une personne est proche du routeur, plus le signal Wi-Fi est puissant. Installer le routeur devant une fenêtre pourrait permettre à des inconnus ou à des cybercriminels de s'y connecter plus facilement!



Jeu 4 : Hameçonnage – la chasse aux indices



Regarde! Nous venons de recevoir plusieurs indices. On pourrait les utiliser pour attraper Viro.

Oh, non! On dirait que les cybercriminels de Viro nous envoient des messages d'hameçonnage pour tenter de nous tromper. Les cybercriminels envoient des messages d'hameçonnage pour faire semblant d'être quelqu'un d'autre. Mais certains d'entre eux ne sont pas très brillants. Parfois, ils font des erreurs facilement reconnaissables, par exemple en utilisant des images floues ou une adresse courriel bizarre. Ensemble, nous pouvons déjouer leur plan!

Regardons ces indices et tentons de différencier ceux qui sont vrais de ceux qui sont une tentative d'hameçonnage. Prêt(e)?

Formation de cyberagent – hameçonnage

Instructions :

Réponds aux questions suivantes en encerclant la bonne réponse. Tu trouveras la solution à toutes les questions du jeu-questionnaire au verso du cahier!

Question 1 : Si tu reçois un message d'un étranger qui te demande de télécharger un fichier, que dois-tu faire?

A Demander l'aide d'un adulte de confiance et supprimer le message.

B Ouvrir le fichier. Quelle est la pire chose qui pourrait se produire?

C Transférer le message à une autre personne.

Indice : Les messages envoyés par des inconnus peuvent être très dangereux!

Question 2 : Vrai ou faux? Des gens sur Internet peuvent tenter de se faire passer pour une autre personne. Certaines personnes essayent ainsi de tromper les autres.

A Vrai.

B Faux.

Indice : Il ne faut pas faire confiance à toutes les personnes que tu rencontres en ligne.

Question 3 : Quels indices peux-tu rechercher pour repérer une tentative d'hameçonnage?

A Les fautes d'orthographe.

B Une adresse de courriel bizarre.

C Des liens suspects et des pièces jointes suspectes.

A Toutes ces réponses.

Indice : Les cybercriminels font parfois des erreurs qui nous indiquent que le message est peut-être un faux message.
Ne clique jamais sur quelque chose qui te semble un peu bizarre.
Indice : Les cybercriminels pourraient te demander de dévoiler des informations personnelles comme ton adresse ou ton mot de passe.
Personne ne devrait te demander ce type d'information dans un message en ligne.

Jeu 4 : La chasse aux indices

Superbe travail, Cyberagent! Maintenant que tu sais comment reconnaître un message d'hameçonnage, voyons comment nous pouvons, ensemble, détecter certains indices dans les messages que nous avons reçus par courriel.

Ces indices importants nous révèlent le plan diabolique de Viro. Mais il semble que ces indices sont mélangés avec des messages d'hameçonnage envoyés par Viro.

Travaillons ensemble afin de distinguer les indices réels des messages d'hameçonnage dangereux.

Comment jouer

- → Lis attentivement chacun des courriels ci-dessous. Entoure ceux qui te semblent être de l'hameçonnage afin que Cybot sache lesquels il doit supprimer plus tard.
- → Réfère-toi à la liste des **indices d'hameçonnage** ci-dessous pour savoir comment différencier les courriels d'hameçonnage et le courriel qui contient un indice à propos du plan diabolique de Viro.
- → Une fois que tu as terminé, tourne la page pour voir si tu as trouvé les bonnes réponses!

Indices d'hameçonnage

Indice no 1 :

Un message qui te demande de faire quelque chose rapidement.

Par exemple : « Cliquez sur ce lien tout de suite avant qu'il ne soit trop tard! »

Indice no 2 :

Un message qui te demande des informations personnelles.

Par exemple : « Veuillez cliquer sur ce lien et nous envoyer votre mot de passe pour vérifier votre compte. »

Indice no 3 :

Un message qui t'informe que tu as gagné de l'argent, un prix ou un concours.

Par exemple : « Félicitations! Vous avez gagné des vacances gratuites à Hawaï! Veuillez nous envoyer 50 $ pour réclamer vos billets. »

Indice no 4 :

Un message qui est rempli de fautes d'orthographe, que ce soit dans l'adresse courriel, le texte ou les liens.

Par exemple :
De : Uwhber231mKn56@boiteauxlettres.com

Message : Bonjourr je vous envoua un mèsage pour un carte cadeau amazone, répondé vite! Clikez

ici : aamazone.com.

Indice no 5 :

Un message qui provient d'une adresse inconnue et qui comporte des pièces jointes bizarres, comme des fichiers, des images ou des dossiers.

Par exemple : « Veuillez télécharger le fichier ci-joint CeciNestPasUnVirus.bat. »

Indce no 6 :

Un message qui contient des images floues ou un design bizarre.

A

À : Agent@Cybersecurite.com

De : SuperAlex@Amis.com

Objet : Ligne d'assistance en cybersécurité

Bonjour Cyberagent,

J'ai entendu dire que Viro préparait une cyberattaque majeure en utilisant un maliciel.
Je n'ai pas d'autres informations pour l'instant. J'espère que cet indice te sera utile.

B

À : Agent@Cybersecurite.com

De : JeNeSuisPasViro@PlansDiaboliques.com

Objet : Le meilleur indice du monde!! 1 !

Alloooo, cyberageeent. Je c où Viro se cache!

Tu peux juss cliqué sur le lien ci-dessous ! Mintenant! et tu pourras le déccouvrir!

[>>**CLIQUE ICI**<<]

C

À : Agent@Cybersecurite.com

De : Attaque@PlansDiaboliques.com

Objet : !Vacances GRATUITES!

Félicitations Cyberagent!!!

Tu as gagné un PRIX! Un voyage tous frais payés aux îles Fidji!
Ne t'inquiète pas pour Viro! Fais tout de suite tes valises!

Clique sur le lien ci-dessous pour envoyer 5 $ afin de réclamer tes billets!!!! Dépêche-toi! L'offre se termine bientôt!

[>>>**Clique ici**<<<]

D

À : Agent@Cybersecurite.com

De : Mechant@Cibersecurite.ca

Objet : Besoin d'aide!!!

Salut!!

Je suis un nouveau cyberagent. J'ai perdu mon mot de passe et je dois emprunter celui de quelqu'un d'autre jusqu'à ce que je retrouve le mien. Est-ce que quelqu'un peut répondre à ce courriel et m'envoyer son mot de passe afin que je puisse l'utiliser? Merci!!

Answers:

A Bonne réponse!

Ce message est sûr. L'expéditeur ne nous fait pas de demande suspecte et ne nous invite pas non plus à cliquer sur quoi que ce soit. Gardons cet indice.

B Oups!

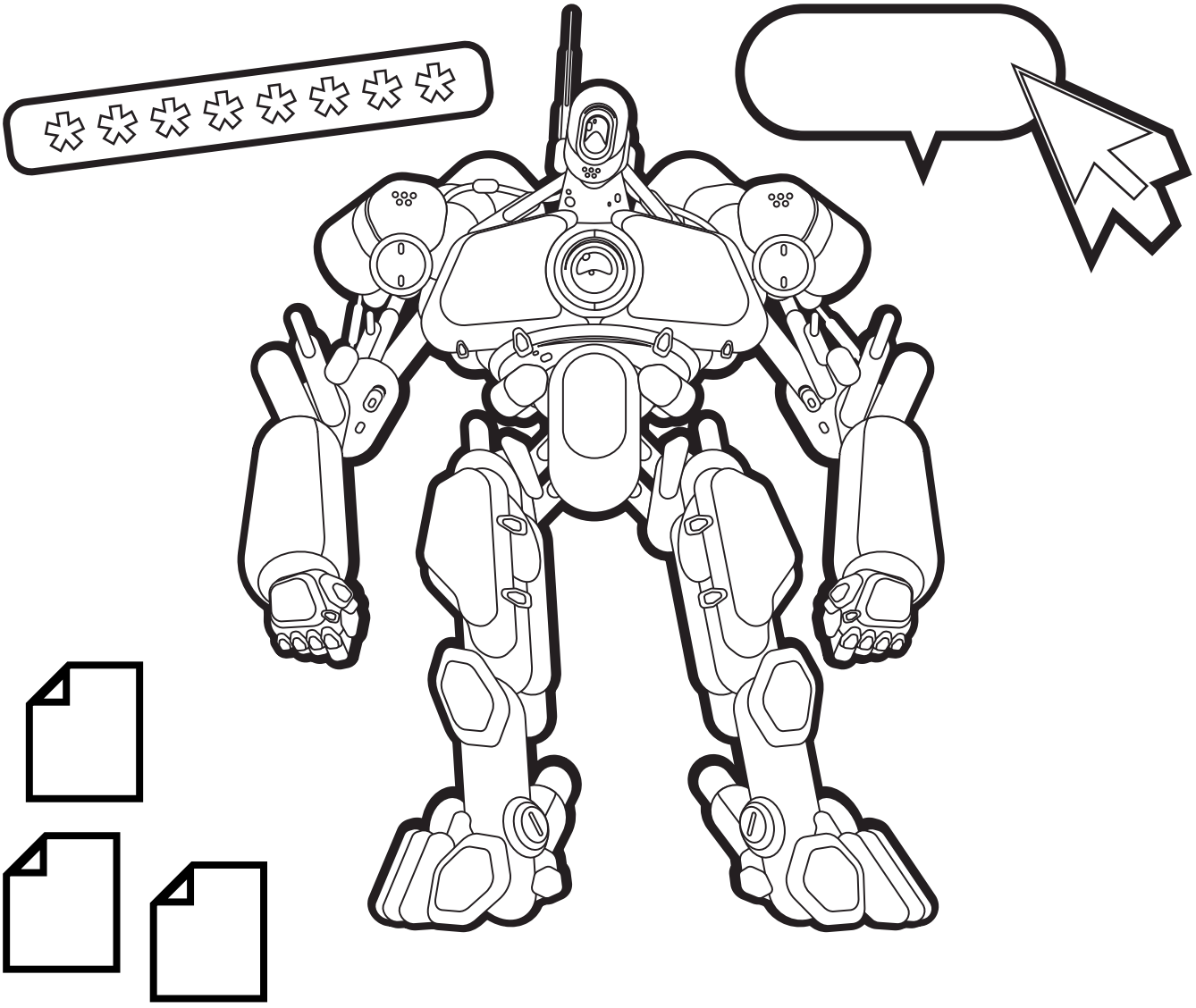
Ce message contient plusieurs fautes d'orthographe ainsi qu'un lien suspect. Utilise **les indices d'hameçonnage** pour reconnaître les messages qui sont des tentatives d'hameçonnage!

C Oups!

On dirait que la personne qui a écrit ce message veut nous amadouer avec un faux prix. Utilise **les indices d'hameçonnage** pour reconnaître les messages qui sont des tentatives d'hameçonnage!

D Oups!

La personne qui a envoyé ce message fait une demande louche. Utilise **les indices d'hameçonnage** pour reconnaître les messages qui sont des tentatives d'hameçonnage!



Jeu 5 : Maliciel – la revanche du maliciel

Mmmm… Bizarre! Je ne peux plus ouvrir mes fichiers! J'ai probablement cliqué sur un courriel d'hameçonnage par erreur! C'est Viro qui a dû nous transmettre un maliciel! Il faut que nous nous en débarrassions tout de suite. Une fois que ce sera fait, tu pourras accéder aux fichiers dont nous avons besoin pour vaincre Viro.

Pour résoudre l'affaire, nous devons décoder un message secret. Mais avant, nous devons comprendre ce qu'est un maliciel afin de vaincre Viro une bonne fois pour toutes!

Formation du cyberagent – maliciel

Instructions :

Réponds aux questions suivantes en encerclant la bonne réponse. Tu trouveras la solution à toutes les questions du jeu-questionnaire au verso!

Question 1 : Vrai ou faux? Faire une sauvegarde de tes données te permet de les récupérer si jamais tu télécharges accidentellement un rançongiciel!

A Vrai.

B Faux.

Indice : Un rançongiciel est un maliciel créé par les cybercriminels. Si tu le télécharges, il bloque l'accès à ton appareil, ce qui permet alors au cybercriminel de te demander de lui envoyer de l'argent pour que tu puisses récupérer tes données.
Indice : Sauvegarder tes données signifie faire une copie de toute l'information qui se trouve dans ton appareil, comme des films, des jeux, des photos ou d'autres fichiers importants.

Question 2 : Un maliciel est un logiciel créé par des cybercriminels pour compromettre :

A Tes données.

B Tes appareils.

C Tes réseaux.

D Toutes ces réponses.

Indice : Un maliciel est un logiciel malveillant. Il peut entrer dans ton appareil lorsque tu télécharges un fichier ou que tu cliques sur un lien.

Question 3 : Quand peux-tu télécharger des fichiers en ligne en toute sécurité?

A Lorsque je reçois un courriel ou un message texte qui me demande de télécharger quelque chose.

B Lorsqu'un adulte en qui j'ai confiance me dit que je peux le faire ou lorsqu'il s'agit d'un site sur lequel j'ai déjà téléchargé un fichier sans problème.

C Lorsque le fichier à télécharger me semble cool.

Indice : On peut télécharger certains fichiers en toute sécurité, mais pas n'importe quel fichier!
Indice : Un fichier à télécharger peut contenir un virus, et parfois on ne s'en aperçoit pas. Il est préférable d'être prudent(e) plutôt que d'être victime!

Jeu 5 : La revanche du maliciel

Beau travail, Cyberagent! Maintenant que tu en sais plus sur les maliciels, essayons de décoder le message secret qui nous permettra de récupérer les fichiers auxquels je n'ai plus accès.

Comment jouer

- → Pour décoder le message secret, inscris les lettres auxquelles chaque chiffre correspond dans les espaces vides ci-dessous.
- → Lorsque tu auras placé toutes les lettres, tu pourras lire le message secret qui t'indiquer a comment récupérer les fichiers que Viro a volés à Cybot!
- → Une fois que tu auras trouvé le message secret, consulte la page suivante!

8	**14**	**16**	**7**	**2**	**13**	**14**	**3**	**10**	**2**

19	**2**	**8**		**17**	**11**	**1**	**20**	**11**	**2**	**3**	**8**

A = 14	F = 17	L = 15	S = 8
B = 5	G =13	N = 18	T = 19
C = 1	H = 20	O =12	U = 16
D = 10	I = 11	P = 9	V = 7
E = 2	K = 4	R = 3	Y = 6

Message secret :

Sauvegarde tes fichiers

Bravo, Cyberagent!

Wow, tu as réussi à décoder le message secret! Il semble que ce soit « **Sauvegarde tes fichiers** ».

Bonne nouvelle! J'ai utilisé un disque dur pour sauvegarder et stocker tous mes fichiers importants, y compris tous ceux dont tu avais besoin pour accomplir ta mission! Maintenant que nous détenons toutes ces connaissances top secrètes, Viro ne peut plus rien contre nous, et nous pouvons empêcher notre centrale d'être victime d'une attaque de maliciels.

Maintenant que tu es un expert en cybersécurité, tu peux utiliser tes connaissances pour protéger ta famille des cybercriminels comme Viro.

Demande l'autorisation d'un adulte de confiance pour visiter le site Web PensezCybersecurite.ca/Enfants et découvrir les autres choses que tu peux mettre en place pour assurer ta cybersécurité dès aujourd'hui!

Réponses aux jeux-questionnaires

Jeu-questionnaire 1 : Les mots de passe et phrases de passe

Question 1

A Bonne réponse!

Tu ne devrais jamais partager tes mots de passe avec quiconque, sauf s'il s'agit d'un adulte de confiance. On ne sait jamais qui pourrait les partager avec quelqu'un d'autre, il est donc préférable de les garder secrets.

B Essaye encore.

Tu peux partager beaucoup de secrets avec tes meilleur(e)s ami(e)s, mais pas tes mots de passe! Ces derniers garantissent ta sécurité en ligne, il est donc important de ne pas les partager avec qui que ce soit.

C Essaye encore.

Un(e) vrai(e) ami(e) ne devrait jamais te demander tes mots de passe, car il n'y a pas de bonnes raisons pour que tu les lui donnes. Tes mots de passe garantissent ta sécurité en ligne, il est donc important de ne pas les partager avec qui que ce soit.

Question 2

A Essaye encore.

Utiliser le même mot de passe pour plusieurs comptes différents n'est pas sécuritaire. Si des cybercriminels découvraient ton mot de passe, ils pourraient pirater tous tes comptes.

Tu peux demander à un adulte de confiance de t'aider à mémoriser tes mots de passe avec un gestionnaire de mots de passe.

B Bonne réponse!

Tu ne dois pas utiliser le même mot de passe pour plusieurs comptes différents. Si les cybercriminels découvraient ton mot de passe, ils pourraient pirater tous tes comptes.

Question 3

A Bonne réponse!

Les phrases de passe sont un type de mot de passe plus long et plus robuste, en plus d'être plus faciles à mémoriser qu'une série de chiffres et de lettres aléatoire.

B Essaye encore.

Les mots de passe courts sont peut-être plus faciles à retenir, mais ces derniers te protègent beaucoup moins bien lorsque tu utilises Internet. Il vaut mieux utiliser une phrase de passe ou un mot de passe plus long à la place.

C Essaye encore.

Le nom de ton animal de compagnie est facile à retenir, mais les cybercriminels peuvent le deviner facilement. Tu ne devrais jamais utiliser des renseignements qui te concernent dans un mot de passe, que ce soit le nom de ton animal de compagnie ou ta date de naissance.

Jeu-questionnaire 2 : Les outils

Question 1

A Essaye encore.

Le fait de sauvegarder un fichier deux fois sur le même appareil ne le protègera pas si tu perds l'appareil, si tu te le fais voler ou s'il se brise. Tu devrais sauvegarder un fichier ailleurs, dans un endroit sécuritaire.

B Bonne réponse!

La meilleure façon de sauvegarder un fichier est de l'enregistrer dans un autre endroit sécuritaire, comme une clé USB, un disque dur ou dans le nuage. Comme ça, si quelque chose arrive à ton appareil, tu conserveras une copie de ton fichier!

C Essaye encore.

Ne supprime pas tes fichiers importants, sinon tu les perdras! Essaye de les sauvegarder ailleurs.

Question 2

A Bonne réponse!

En plus d'utiliser une phrase de passe, tu peux recourir à l'authentification multifactorielle sur tes comptes et tes appareils lorsque tu t'y connectes. L'authentification multifactorielle est une étape additionnelle qui permet de vérifier ton identité, par exemple avec la reconnaissance faciale ou avec un code de sécurité!

B Essaye encore.

C'est vrai que l'authentification multifactorielle, c'est deux mots très longs! Mais en réalité, c'est avant tout une excellente manière de te protéger toi, mais aussi de protéger tes comptes et tes appareils.

C Essaye encore.

Non, l'authentification multifactorielle n'est pas une énigme! Elle a pour but de rendre beaucoup plus difficile l'accès à tes comptes pour les cybercriminels! L'authentification multifactorielle est un excellent moyen de te protéger toi, mais aussi de protéger tes comptes et tes appareils.

Question 3

A Bonne réponse!

Tu devrais mettre à jour tes logiciels aussi souvent que possible pour garantir la sécurité de tes appareils. Demande à un adulte de confiance de t'aider à activer les mises à jour automatiques, afin que tes appareils se mettent à jour tout seuls!

B Essaye encore.

Si ton téléphone ou un autre de tes appareils est super lent, c'est peut-être le signe qu'il a besoin de mises à jour logicielles. N'attends pas que tes appareils ralentissent pour les mettre à jour!

C Essaye encore.

Quelle est la manière la plus simple de se débarrasser d'un message de rappel? Exécuter la mise à jour du logiciel, bien sûr! Plus vite tu effectueras la mise à jour, plus vite la fenêtre de rappel disparaîtra.

Jeu-questionnaire 3 : Wi-Fi/Réseaux

Question 1

A Bonne réponse!

Les mises à jour logicielles assurent la sécurité de tes appareils. Lorsque ces derniers sont protégés, tout ce à quoi ils sont connectés l'est aussi, y compris ton réseau Wi-Fi!

B Essaye encore.

La mise à jour de tes appareils est un des meilleurs moyens pour assurer ta cybersécurité !

Question 2 :

A Essaye encore.

Si tu installes ton routeur près des murs extérieurs de la maison, des inconnus ou des cybercriminels pourraient se connecter à ton réseau Wi-Fi plus facilement! Sache que plus tu es proche du Wi-Fi, plus le signal il est puissant. Il est donc préférable de placer le routeur plus près de l'endroit où tu te trouves.

B Bonne réponse!

En installant ton routeur au centre de la maison, il sera plus facile pour toi et ta famille de vous connecter au réseau Wi-Fi et plus difficile pour les cybercriminels d'y accéder!

C Essaye encore.

Cacher des choses peut parfois être un bon moyen de les garder en sécurité, mais pas lorsqu'il s'agit d'un routeur! Si ton routeur est enterré sous tes jouets ou caché quelque part, il peut être difficile pour toi et ta famille de vous connecter au Wi-Fi!

Question 3

A Essaye encore.

Bien que cette réponse soit correcte, il ne s'agit pas de la seule bonne raison. Il y a une autre réponse encore meilleure.

B Essaye encore.

Bien que cette réponse soit correcte, il ne s'agit pas de la seule bonne raison. Il y a une autre réponse encore meilleure.

C Bonne réponse!

Beaucoup de routeurs possèdent le même mot de passe intégré, que les cybercriminels peuvent facilement trouver. Demande à un adulte de confiance s'il a changé le mot de passe du Wi-Fi.

Jeu-questionnaire 4 : Hameçonnage

Question 1

A Bonne réponse!

Il ne faut jamais ouvrir les messages d'inconnus ni cliquer sur des liens bizarres ou sur les téléchargements suspects. La meilleure chose à faire est de ne rien toucher, de demander à un adulte de confiance de t'aider et de supprimer le message.

B Essaye encore.

Ouvrir un message provenant de quelqu'un que tu ne connais pas peut être dangereux. Tu pourrais télécharger un virus par accident, ou pire encore!

C Essaye encore.

Tu ne devrais jamais transférer un message qui te semble bizarre à quelqu'un d'autre! L'envoi d'un mauvais message à un(e) ami(e) ou à un membre de ta famille pourrait lui transmettre un virus ou lui faire perdre ses données personnelles. La meilleure chose à faire est de demander à un adulte de confiance de t'aider et de supprimer le message.

Question 2

A Bonne réponse!

Beaucoup de gens gardent leur identité secrète en ligne et se font passer pour quelqu'un qu'ils ne sont pas. Si tu n'es pas sûr(e) qu'une personne est bien celle qu'elle prétend être, demande à un adulte de confiance de t'aider.

B Essaye encore.

Il peut être difficile de savoir si une personne est bel et bien celle qu'elle prétend être sur Internet, car on ne peut pas la voir dans la vraie vie! Certains individus se feront passer pour des personnes que tu connais. Si tu n'es pas sûr(e), demande à un adulte de confiance de t'aider.

Question 3

A Essaye encore.

Bien que les fautes d'orthographe soient l'une des erreurs les plus courantes des cybercriminels, ce n'est pas le seul indice. Il y a une autre réponse encore meilleure.

B Essaye encore.

Les cybercriminels utilisent souvent des adresses électroniques composées de lettres et de chiffres aléatoires ou même leur adresse électronique personnelle pour essayer de tromper les gens, mais ce n'est pas le seul indice. Il y a une autre réponse encore meilleure.

C Essaye encore.

Les cybercriminels veulent que tu cliques sur des liens ou des pièces jointes bizarres pour obtenir des informations auprès de toi ou te forcer à télécharger quelque chose de dangereux, par exemple un virus, mais ce n'est pas le seul indice. Il y a une autre réponse encore meilleure.

D Bonne réponse!

Les fautes d'orthographe, une adresse électronique étrange ainsi que des liens et des téléchargements bizarres sont autant de signes qui te permettent de reconnaître une tentative d'hameçonnage. Reste sur tes gardes lorsque tu reçois un message de quelqu'un que tu ne connais pas!

Jeu-questionnaire 5 : Maliciel

Question 1

A Bonne réponse!

La sauvegarde de tes données hors ligne est un excellent moyen de conserver tes fichiers les plus importants si jamais tu les perds ou te les fais voler.

B Essaye encore.

La sauvegarde de tes données hors ligne te permet de conserver tes fichiers. En effet, puisqu'une copie de tous tes fichiers importants est sauvegardée ailleurs, ces derniers ne seront pas affectés : tu pourras toujours les restaurer. Autrement dit, tu ne risques pas de les perdre!

Question 2

A Essaye encore.

Un maliciel peut supprimer ou voler tes données. Mais les données ne sont pas les seules choses qu'un maliciel peut compromettre.

B Essaye encore.

Un maliciel peut endommager tes appareils, par exemple les rendre plus lents. Mais les appareils ne sont pas les seules choses qu'un maliciel peut compromettre.

C Essaye encore.

Un maliciel peut accéder à ton réseau pour voler tes données ou infecter tes appareils. Mais les réseaux ne sont pas les seules choses qu'un maliciel peut compromettre.

D Bonne réponse!

Un maliciel est un logiciel malveillant qui peut nuire aussi bien à tes données qu'à tes appareils et à ton réseau.

Question 3

A Essaye encore.

Tu ne devrais jamais télécharger quelque chose que tu reçois par courriel ou par message texte, surtout si tu ne connais pas la personne qui te l'envoie! Demande à un adulte de confiance de t'aider et supprime le message.

B Bonne réponse!

Tu devrais toujours demander l'avis d'un adulte de confiance avant de télécharger quoi que ce soit en ligne.

C Essaye encore.

Même si quelque chose semble cool à télécharger, ça ne veut pas dire que c'est le cas. Avant de télécharger quoi que ce soit, demande la permission à un adulte de confiance.

Glossaire

Logiciel antivirus

Type de logiciel spécialement conçu pour protéger tes appareils contre les virus informatiques. Les logiciels antivirus sont capables de détecter les programmes malveillants qui peuvent se trouver sur ton ordinateur.

Pièce jointe

Fichier que tu peux télécharger. La pièce jointe peut contenir des fichiers sûrs, par exemple des images, des vidéos ou des documents, mais elle peut aussi contenir des fichiers dangereux comme des maliciels et des virus.

Sauvegarde

Faire une ou plusieurs copies additionnelles de données, par exemple des fichiers ou des logiciels, au cas où l'original serait perdu ou endommagé.

Stockage infonuagique

Moyen d'enregistrer des fichiers, des documents et des photos sur un serveur qui n'est pas sur ton appareil ou à proximité. Un service de stockage en nuage peut être fourni avec ton ordinateur ou ton appareil.

Appareil

Outil électronique comme un téléphone, ordinateur portable ou tablette, que tu peux utiliser à la maison.

Téléchargement

Envoi et réception de données d'un appareil à l'autre.

Pare-feu

Barrière de sécurité aidant à protéger tes appareils des personnes qui pourraient tenter d'y accéder.

Disque dur (externe)

Dispositif que tu branches à ton ordinateur et dans lequel tu peux stocker ou sauvegarder des données.

Maliciel

Logiciel malveillant créé par les cybercriminels pour endommager les ordinateurs. Les maliciels peuvent compromettre tes appareils, que ce soit en volant des informations, en supprimant des éléments importants ou en se faisant passer pour toi.

Authentification multifactorielle

Étape de sécurité supplémentaire pour te connecter à tes comptes et à tes appareils. L'authentification multifactorielle nécessite des informations additionnelles qui permettent de vérifier ton identité : empreinte digitale; reconnaissance faciale; code secret de type NIP. L'objectif est ainsi d'empêcher les cybercriminels d'accéder à tes comptes et à tes appareils.

Réseau

Connexion entre plusieurs appareils, par exemple un routeur, un téléphone et un ordinateur portable.

Phrase de passe

Combinaison de mots aléatoires que tu choisis pour sécuriser un compte ou un appareil.

Mot de passe

Combinaison de lettres et de chiffres que tu choisis pour sécuriser un compte ou un appareil.

Gestionnaire de mots de passe

Outil conçu pour stocker tous tes mots de passe et phrases de passe, afin de ne pas avoir à tous les mémoriser toi-même. Cet outil peut également t'aider à assurer la sécurité de tes mots de passe et tes phrases de passe.

NIP

Numéro d'identification personnel. Il s'agit d'un code d'accès composé uniquement de chiffres et qui fonctionne comme un mot de passe ou une phrase de passe lorsque tu souhaites accéder à un compte ou à un appareil.

Hameçonnage

Tentative opérée par les cybercriminels pour voler des renseignements personnels à un individu, un groupe ou une organisation en se faisant passer pour une marque, généralement bien connue. Autrement dit, l'hameçonnage se produit lorsque des cybercriminels t'envoient un message pour te voler des renseignements ou de l'argent. Ils se font alors passer pour quelqu'un qu'ils ne sont pas afin de t'inciter à leur transmettre des informations te concernant.

Routeur

Un petit appareil qui permet aux autres appareils, comme les tablettes électroniques et les téléphones, de se connecter à Internet.

Logiciel

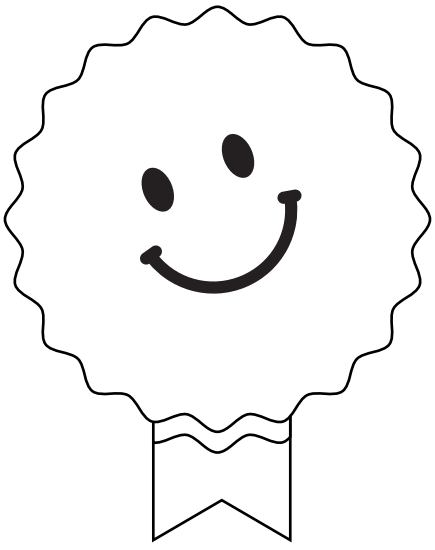
Programme informatique permettant à tes appareils de fonctionner. Tu connais probablement déjà les logiciels courants que sont Windows, Linux ou Mac. Un logiciel peut également être une application, comme Microsoft Word ou iMovie.

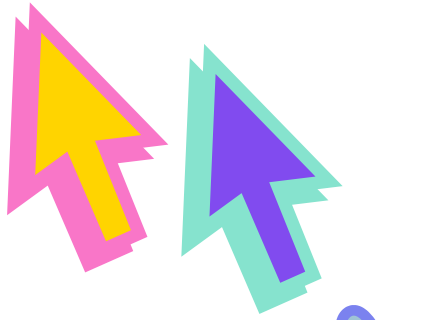
Mise à jour

Processus permettant d'ajouter de nouvelles fonctionnalités et de corriger les bogues ou les erreurs sur les logiciels et les appareils. Souvent, les mises à jour procurent à tes appareils de nouvelles fonctions de sécurité pour les protéger des cyberattaques.

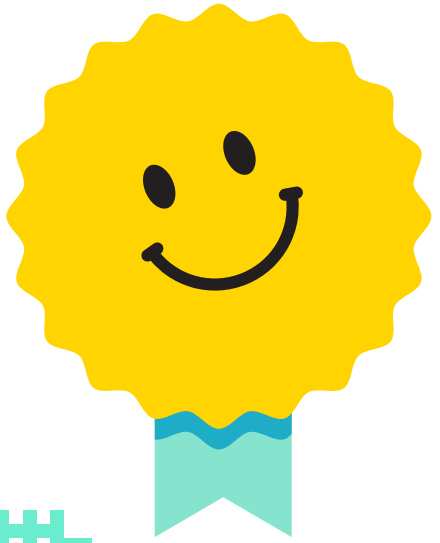
Wi-Fi

Technologie de transmission sans fil permettant de connecter à Internet tes appareils, comme un ordinateur portable, une tablette et un téléphone. L'utilisation du Wi-Fi à la maison est généralement assez sûr puisque le réseau est protégé. Tu ne devrais jamais connecter un de tes appareils à un Wi-Fi public — comme au centre commercial ou dans un cafésans la permission d'un adulte de confiance.





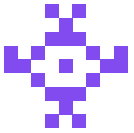
Certificat de cybersécurité

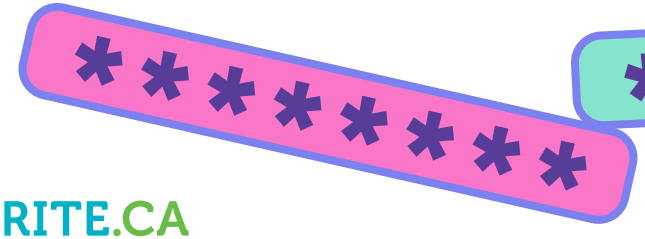


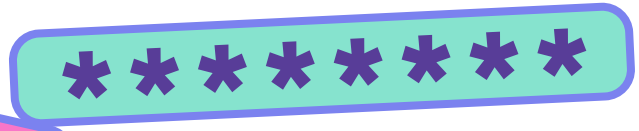
Ce certificat est remis avec fierté à :

_____

pour avoir complété sa formation de cyber agent.







PENSEZCYBERSECURITE.CA

Canada