Quand ta mère te dit que la cybersécurité est une perte de temps.

Recevoir un courriel d'un parent perdu de vue qui demande de l'argent.

Envoyer à ta flamme un message direct, et te rendre compte que c'est un bot.

Recevoir un message texte d'un numéro inconnu qui dit que tu as gagné à la loto.

Quand le gouvernement du Canada t'envoie un message texte pour te réclamer de l'argent.

Utiliser le même mot de passe facile pour tout.

Quand ton ami est victime d'hameçonnage par message texte.

Quand tu envoies 1 000 $ à un prince étranger et il ne te rappelle pas.

Cliquer sur Mettre à jour plus tard 200 fois et votre ordinateur sonne comme un lave-auto.

Tenter d'utiliser l'empreinte de patte de ton chat comme 3e facteur d'authentification.

Utiliser le compte Netflix de ton ex parce qu'il ne change jamais son mot de passe.

Utiliser un gestionnaire de mot de passe et oublier le mot de passe pour y accéder.

Quand ton cousin pense avoir gagné un voyage en *Italiee*, mais tu as reçu le même courriel.

Quand tu demandes à ton père s'il a reçu un courriel d'hameçonnage et il sort sa canne à pêche.

Oublier les réponses à tes questions de sécurité.

Tenter de créer un mot de passe unique qui ne contient pas le nom de ton chien.

Essayer de savoir si c'est une tentative d'hameçonnage ou s'il s'agit bien de ton relevé de compte.

Recevoir un courriel pour réinitialiser le mot de passe d'un compte que tu n'as jamais eu.

Quand le soutien technique te demande si tu as essayé de fermer ton appareil, puis de le rouvrir.

Dire aux TI que ton ordi est brisé, mais lorsqu'ils l'examinent, il fonctionne bien.

S'emporter contre un agent de télémarketing en croyant que c'est une tentative d'hameçonnage.

Dire « merci » et « s'il te plait » à ton haut-parleur intelligent pour éviter une révolte de robots.

Personnaliser tes réglages de sécurité des réseaux sociaux pour cacher tes vieilles photos embarrassantes.

Quand ton meilleur ami te parle de sauvegarde, mais tu crois qu'il pense à ta réputation...

Installer un antivirus, mais ne jamais le mettre à jour.

Quand une fenêtre contextuelle agaçante clignote au rythme de la chanson que tu écoutes.

Quand ton ami te rembourse en utilisant le réseau Wi-Fi d'un café.

Constater que tu ne seras jamais victime d'hameçonnage si tu ne prends jamais tes courriels.

Quand le message d'hameçonnage contient ton vrai nom pour t'amadouer.

Quand le lien pour obtenir des monnaies de jeu gratuites te donne un virus coûteux.

Se rendre compte que le RPV ne sert pas uniquement à t'abonner à des services de diffusion en direct étrangers.

Activer un coupe-feu pour réchauffer la pièce.

Un commerçant en ligne te demande ton numéro d'assurance sociale pour la livraison.

Créer un mot de passe qui ne contient pas le nom de ton chien ou d'un membre de la famille.

Quand ton ami se connecte au réseau invité que tu as créé.

Mettre à jour ton ordinateur dès que tu y es invité.

Vérifier l'adresse de l'expéditeur d'un courriel suspect.

Décocher la case « Se souvenir de mes renseignements de connexion » après s'être connecté.

Activer la mise à jour automatique de tes logiciels.

Installer un nouveau logiciel de cybersécurité.

Moi, éclairant mes amis sur les vertus des phrases de passe.

Lire la politique de confidentialité avant de télécharger une application.

Recevoir un courriel suspect et le supprimer sur-le-champ.

Quand les mises à jour automatiques sont activées et s'installent d'elles-mêmes durant la nuit.

Recevoir un message texte d'hameçonnage et bloquer l'expéditeur.

Changer le nom par défaut de ton routeur pour le rendre unique.

Quand ton navigateur demande de sauvegarder ta carte de crédit et tu cliques sur « Non merci ».

Quand tu oublies un de tes mots de passe, mais tu utilises un gestionnaire de mot de passe.

Créer un réseau secondaire pour tous tes appareils intelligents.

Utiliser un RPV pour se connecter à un réseau Wi-Fi public.

Utiliser un mot de passe unique pour chacun de tes comptes.

Activer l'authentification multifactorielle au cas où quelqu'un devinerait ton mot de passe.

Quand tu as enfin le temps de personnaliser les paramètres de confidentialité de tes comptes de réseaux sociaux.

Mettre à jour ton appareil et découvrir plein de nouvelles fonctionnalités.

Quand tu mets à jour ton application préférée et elle arrête enfin de t'embêter.

Enfin découvrir le logiciel antivirus qui répond parfaitement à tes besoins.

Changer le mot de passe par défaut de ton routeur pour une phrase de passe robuste.

Sauvegarder tes données chaque semaine de façon à les protéger en cas de perte.

Envoyer un courriel à ton collègue pour confirmer qu'il veut que tu achètes 20 cartes-cadeaux.

Désinstaller l'appli de calculatrice qui exige l'accès à ta caméra, à ton micro et à ta localisation.

Désactiver la géolocalisation de ton appareil photo pour éviter qu'on te localise.

Contrevérifier les notifications de ton compte avant de répondre à un courriel d'hameçonnage.

Quand tu vérifies les caractéristiques de sécurité d'un appareil avant de l'acheter.

Recouvrir la caméra Web de ton ordinateur portable après un appel vidéo.

Supprimer ton historique de navigation et les témoins.

Quand ton nom d'utilisateur ne contient aucun renseignement personnel.

Déconnecter tous tes vieux appareils Bluetooth.

Cliquer sur « Non » à chaque fois que ton navigateur veut sauvegarder tes données de connexion

Télécharger sur-le-champ les mises à jour de ta nouvelle tablette reçue en cadeau.

Quand tu affiches tes projets de voyage des fêtes et ta famille n'est pas invitée.

Quand un membre de ta famille te demande pourquoi tu es toujours célibataire.

Quand ton compte est piraté et tous voient quel cadeau tu leur as acheté.

Quand tu fais jouer le disque des Fêtes de Michael Bublé chaque fois que possible.

Quand tu installes tes décorations des Fêtes dès le 1er novembre à minuit une minute.

Quant tu magasines pour des cadeaux et tu commences par les tiens.

Vacances des Fêtes en famille : Jour 3

Bar ouvert à la fête du bureau.

Retour au bureau après le temps des fêtes...

Constater que les vacances des Fêtes sont pratiquement terminées.

Quand les Fêtes approchent et tu commences à participer aux préparatifs.

Quand tu dis à quelqu'un que son cadeau de Noël, c'est toi!

Revenir de vacances et avoir oublié comment faire ton travail.

Recevoir un code promo avec un rabais de 50 % pour ce pull que tu aurais acheté de toute façon.

Mon service de diffusion en continu: « êtes-vous toujours là? »
Moi :

Mon estomac après ma première gorgée de café.

Rencontrer enfin l'amour de sa vie et se rendre compte qu'il aime la pizza à l'ananas.

N'importe quel père qui entre dans une quincaillerie.

Ouvrir son micro une seule fois pour dire « D'accord » dans une réunion Zoom.

Quand tu travailles de la maison et on te demande de participer à un appel vidéo.

Moi, délaissant ma liste de choses à faire pour faire une blague irrésistible sur Twitter.

Constater que vivre en quarantaine, c'est devenu la vie normale.

Croiser un collègue que tu ne connais pas vraiment.

Écouter une conversation entre deux étrangers et y participez dans votre tête.

Manger une seule bouchée d'un fruit et se sentir subitement invincible.

Écouter un enregistrement de sa propre voix.

Recevoir un appel et attendre que la sonnerie cesse pour pouvoir utiliser ton téléphone à nouveau.

Dire « Merci, vous aussi » au livreur qui te dit : « Bon appétit ».

Tenter de demeurer positif au bureau.

Quand tu tentes d'avaler un comprimé, mais celui-ci commence à fondre dans ta bouche.

Quitter la maison à 8 h 55 pour une réunion à 9 h.

Commander un taco et l'échapper par terre.

Cliquer sur « Épisode suivant » et constater que tu as écouté toute la série.

Quand le serveur reprend ton assiette, mais il y avait encore des frites dedans.

Quand tu dis « Belle chemise » à quelqu'un qui porte la même que toi.

Voilà à quoi ressemble le bonheur.

Tous les pères quand on change le réglage du thermostat d'un demi-degré.

Quant on remet une tâche au lendemain... et le lendemain est arrivé.

Eux : Que fais-tu pour t'amuser?
Moi :

Tenter de sortir la nourriture de la gueule du chien.

Boire un grand verre de jus d'orange après s'être brossé les dents.

Se cogner l'orteil sur la patte de ton lit à 3 h du matin.

Quand il te manque 0,10 $ et la caissière te dit que ce n'est pas grave.

Moi : Pourquoi ai-je toujours mal au dos?
Moi aussi :

Quand tu es loin de la maison et la pile de ton téléphone est à 1 %.

Toi, seul à la maison un vendredi soir.

Lire un message texte que tu essayais d'éviter.

Trouver une 11e pépite de poulet dans une boîte de 10.

Quand ton collègue pose une question qui allonge la réunion de 30 minutes.

Quand tu dois rendre un projet à 11 h 59 et Internet tombe en panne à 11 h 58.

Toi au réveil de la sieste.

Quand un ami publie une photo où tu n'es pas à ton avantage, mais lui, oui.

Moi, après avoir monté les escaliers sur trois étages.

Quelqu'un te dit « wow, tu te lèves tôt! » alors que tu as passé la nuit debout.

Ton chien faisant semblant que ce n'est pas lui qui a chipé de la nourriture sur la table.

Quand mes amis me montrent une combinaison de cartes hilarante.

Quand personne ne choisit tes cartes même si tes réponses sont les plus drôles.

Quand tu ouvres la boîte de biscuits de grand-maman, mais elle contient des articles de couture.

Parler d'acheter un nouveau matelas et recevoir une publicité de matelas tout de suite après.

Quand un ami s'effondre en larmes et tu ne sais pas comment le consoler.

Quand quelqu'un tend la main pour serrer la tienne et tu lui fais une accolade.

Je crois toujours que je suis une personne facile d'approche, mais je en fait je ressemble à ça.

Quand ta mère te passe le téléphone pour saluer un parent dont tu n'as jamais entendu parler.

Dire « J'adore » au coiffeur alors que tu détestes ta nouvelle coupe.

Ne pas pouvoir s'endormir parce que tu te rappeles de quelque chose que tu as dit en 3e année.

Regarder une vieille photo de vous.

Quand quelqu'un te dit qu'il aime l'astronomie et tu lui dis que tu es capricorne.

Vérifier ton compte en banque après la fin de semaine.

Quand tu rentres chez toi et tu peux enfin être toi-même.

À l'aide, mon coupe-feu ne fonctionne plus, je ne peux pas redémarrer.

Mon routeur m'a laissé pour une mise à jour micrologicielle.

Tu as partagé ton mot de passe? C'est dégueu.

Ce n'est pas toi, c'est ton mot de passe facile.

Les années 90 viennent d'appeler, elles veulent récupérer leur cryptage faible.

Le lait de poule est expiré, je crois. La date est encodée.

On ne guérit pas le mal par le mal, mais plutôt par l'authentification multifactorielle.

Je n'ai pas utilisé d'antivirus. Maintenant j'ai un cheval de Troie.

Activer un coupe-feu pour réchaufer la pièce.

Oublié les réponces à té questions de sécurité.

Quand ta mère te dit que la cybersécurité est une perte de taon.

Tenter d'utiliser l'empreinte de patte de ton chat **comme 3e facteur d'authentification.**

Installer un antivirus, mais ne jamais le mettre à jour.

Utiliser un gestionnaire de mot de passe, mais oublier le mot de passe pour y accéder.

Quand le lien pour obtennir des monaies de jeu gratuites te done un virus coûteu.

S'emporter contre un agent de télémarketing en croyant que c'est une tentative de pèche.

Cliquer sur Mettre à jour plus tard 200 fois et votre ordinateur sonne comme un lave-auto.

Quand une fenêtre contextuelle agassante clignote au rythme de la chansson que tu écoutes.

Changer le mot de passe par défaut de ton routeur pour une phrase de passe robuste.

Sovegarder vos données chaque semène de façon à les protéger en cas de perte.

Envoyer un courriel à ton collègue pour confirmer qu'il veut que tu achètes 20 cartes-cadeaux.

Installer un nouveau logiciel de cybersécurité ABAT LA CARTE PHOTO MAINTENANT!

Moi, éclairant mes amis sur les virus des phrases de passe.

Lire la politique de confidentialité avant de télécharger une application.

Recevoir un courriel suspé et le supprimer sur-le-champ.

Quand ton nom d'utilisateur ne contient aucun renseignement personnel METTRE À JOUR TES RENSEIGNEMENTS**.**

RÉP: RÉP: RÉP: NOTIFICATION D'ENVOI: Déconnecter tous tes vieux appareils Bluetooth.

Cliquer sur « Non » à chaque fois que ton naviteur veut sauvegarder tes données de connexion.

Quand tu travailles delamaison et on te demande de participer à un appelvidéo.

MOI, DÉLAISSANT MA LISTE DE CHOSES À FAIRE POUR FAIRE UNE BLAGUE IRRÉSISTIBLE SUR TWITTER!!!!

TR: VOTRE REÇU: Constater que vivre en quarantaine, c'est devenu la vie normale.

VOUS AVEZ GAGNÉ! Croiser un collègue que tu ne connais pas RÉCLAMEZ VOTRE PRIX!

Quand un ami publie une phauteau où tu n'es pas à ton avantage, mais lui, oui.

Moi, après avoir monter les escalliers sur trois étages.

Quelqu'un te dit « wow, tu te lèves tôt! » alors que tu as passé la nuit debout.

Ton chien faisant semb1ant que ce n'est pas 1ui qui a chipé de la nourriture sur la tab1e.

Tenter de sortir la nourriture de la gueule du chien PLACEZ UNE CARTE OU VOTRE COMPTE SERA FERMÉ.

Quand ton ami se connecte au réseau invité que tu as créééé.

C'est nul.

C'est nul.

Mettre à la corbeille (ou donner à un autre joueur).

Mettre à la corbeille (ou donner à un autre joueur).

Espérons que ce film que tu as téléchargé en valait la peine.

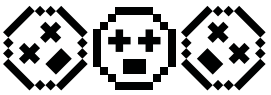
Espérons que ce film que tu as téléchargé en valait la peine.

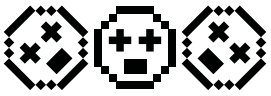
Où est le million de dollars que ce courriel te promettait?

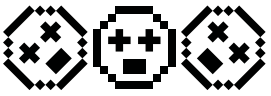
Où est le million de dollars que ce courriel te promettait?

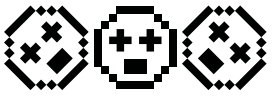
C'est si difficile de mettre à jour ton logiciel antivirus?

C'est si difficile de mettre à jour ton logiciel antivirus?









ÉDUCATION

2 Canadiens sur 5 ont été victimes d'un virus, d'un logiciel espion ou d'un maliciel.

ÉDUCATION

2 Canadiens sur 5 ont été victimes d'un virus, d'un logiciel espion ou d'un maliciel.

ÉDUCATION

70 % des Canadiens disent qu'ils essaient de créer des mots de passe robustes.

ÉDUCATION

70 % des Canadiens disent qu'ils essaient de créer des mots de passe robustes.

ÉDUCATION

46 % des Canadiens activent les mises à jour automatiques.

ÉDUCATION

46 % des Canadiens activent les mises à jour automatiques.

ÉDUCATION

90 % des Canadiens utilisent un mot de passe unique à leur réseau Wi-Fi à domicilei.

ÉDUCATION

90 % des Canadiens utilisent un mot de passe unique à leur réseau Wi-Fi à domicilei.

ÉDUCATION

AUTHENTIFICATION MULTIFACTORIELLE

L'authentification multifactorielle utilise au moins deux facteurs pour vous identifier.

AUTHENTIFICATION MULTIFACTORIELLE

L'authentification multifactorielle utilise au moins deux facteurs pour vous identifier.

AUTHENTIFICATION MULTIFACTORIELLE

L'authentification multifactorielle est offerte sur un grand nombre d'appareils ou de comptes.

AUTHENTIFICATION MULTIFACTORIELLE

L'authentification multifactorielle est offerte sur un grand nombre d'appareils ou de comptes.

AUTHENTIFICATION MULTIFACTORIELLE

L'utilisation de l'empreinte digitale pour accéder à son appareil est un exemple d'authentification multifactorielle.

AUTHENTIFICATION MULTIFACTORIELLE

L'utilisation de l'empreinte digitale pour accéder à son appareil est un exemple d'authentification multifactorielle.

AUTHENTIFICATION MULTIFACTORIELLE

L'authentification multifactorielle ajoute un niveau de sécurité à un mot de passe robuste.

AUTHENTIFICATION MULTIFACTORIELLE

L'authentification multifactorielle ajoute un niveau de sécurité à un mot de passe robuste.

AUTHENTIFICATION MULTIFACTORIELLE

MISES À JOUR LOGICIELLES

Faire régulièrement les mises à jour logicielles est la façon la plus simple de contrer les cybermenaces.

MISES À JOUR LOGICIELLES

Faire régulièrement les mises à jour logicielles est la façon la plus simple de contrer les cybermenaces.

MISES À JOUR LOGICIELLES

Activez la mise à jour automatique sur vos appareils pour ne plus avoir à y penser.

MISES À JOUR LOGICIELLES

Activez la mise à jour automatique sur vos appareils pour ne plus avoir à y penser.

MISES À JOUR LOGICIELLES

Les mises à jour contiennent des rustines de sécurité et des nouvelles fonctionnalités super intéressantes.

MISES À JOUR LOGICIELLES

Les mises à jour contiennent des rustines de sécurité et des nouvelles fonctionnalités super intéressantes.

MISES À JOUR LOGICIELLES

N'attendez pas: faites la mise à jour logicielle dès qu'elle vous est offerte.

MISES À JOUR LOGICIELLES

N'attendez pas: faites la mise à jour logicielle dès qu'elle vous est offerte.

MISES À JOUR LOGICIELLES

@PENSEZCYBERSECURITE
@CYBER_SECURITE

@PENSEZCYBERSECURITE
@CYBER_SECURITE

@PENSEZCYBERSECURITE
@CYBER_SECURITE

@PENSEZCYBERSECURITE
@CYBER_SECURITE

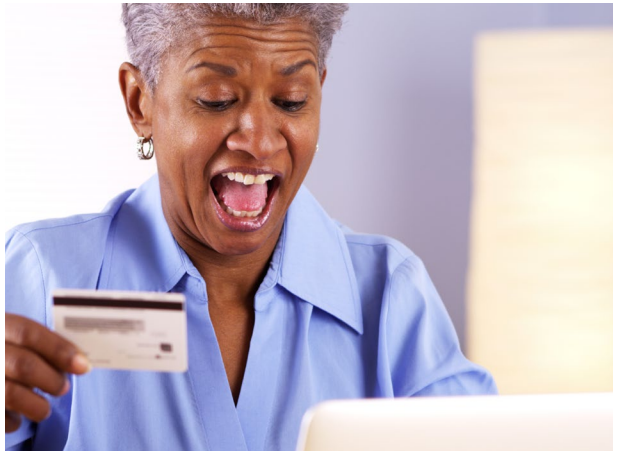
@PENSEZCYBERSECURITE
@CYBER_SECURITE

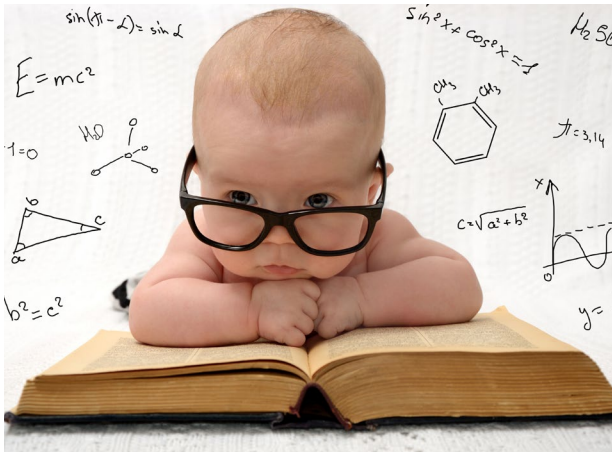
@PENSEZCYBERSECURITE
@CYBER_SECURITE

@PENSEZCYBERSECURITE
@CYBER_SECURITE

@PENSEZCYBERSECURITE
@CYBER_SECURITE

@PENSEZCYBERSECURITE
@CYBER_SECURITE




E=mc²
c=√a²+b²
b²=c²

37
82
125

JE PENSE, DONC JE MÊME: PENSEZ CYBERSÉCURITÉ

Le jeu de société qui vous apprend la cybersécurité

PRÉPARATION

1. Téléchargez et imprimez **ce PDF** pour obtenir vos cartes.

Pour des cartes plus solides, nous recommandons de les faire imprimer chez un imprimeur spécialisé et les faire monter sur carton.

2. Découpez les cartes.

Vous pouvez les découper aux ciseaux, mais un couteau à lame rétractable est préférable.

3. Séparez les diverses catégories de cartes (Légende, Photo, Cybermenace et Cybersécurité).

Les cartes Cybermenace et Légende vont ensemble. Les autres catégories de cartes sont séparées.

PRÉPARATION ALTERNATIVE

Oubliez l'impression des cartes : **jouez en ligne**.

DÉROULEMENT DU JEU

- Chaque joueur pige cinq cartes Légende.
- Le joueur qui a le plus récemment fait la mise à jour de son appareil est le premier à tenir le rôle de juge. Si tous les joueurs ont activé leur mise à jour automatique, c'est le dernier joueur à avoir reçu un courriel d'hameçonnage qui s'exécute en premier. Il serait amusant de lire le courriel d'hameçonnage reçu de façon ironique. Cela ne vaudra aucun point supplémentaire au joueur, mais ajoutera du piquant au jeu.
- Le juge brasse les cartes Photo et retourne la première carte sur la pile.
- Dans leurs cartes Légende, les autres joueurs choisissent celle qui est la plus drôle par rapport à la carte Photo retournée par le juge et la placent face cachée sur la table.
- Le juge prend les cartes remises par les autres joueurs, les brasse et les lit à tour de rôle à voix haute.
- Le juge choisit celle qui, à ses yeux, est la plus drôle et le joueur à qui cette carte appartient remporte la manche et prend la carte Photo.
- Chaque joueur qui a perdu une de ses cinq cartes pigent une nouvelle carte.
- Lorsqu'une manche est terminée, le joueur placé à la gauche du premier juge devient juge pour la manche suivante.
- Le premier joueur à obtenir 10 cartes Photo gagne la partie.

UN PEU DE PIQUANT

Contrairement aux autres jeux de cartes photos, *Je pense, donc je même: Pensez cybersécurité* comporte d'autres catégories de cartes qui ont pour but de semer la zizanie parmi les joueurs, comme seul un grand jeu de société le fait.

CARTES CYBERMENACE

Comme une véritable cybermenace, ces cartes truquées permettent à un joueur de s'emparer de ce qui est aux autres, c'est-à-dire de ses cartes. Il y a deux types de cartes Cybermenace :

CARTES HAMEÇONNAGE

Comme un véritable message d'hameçonnage, ces cartes ressemblent aux cartes Légende, mais elles comportent de petites différences qui permettent de les distinguer. Ces différences sont notamment :

- Demande urgente ou langage menaçant
- Demande de renseignement personnels
- Promesse d'une chose qui est trop belle pour être vraie
- Mises à jour ou réception inattendues
- Fichiers joints suspects
- Graphisme de mauvaise qualité
- Fautes d'orthographe ou de grammaire
- Lien qui mène à un site inattendu

Les cartes Hameçonnage sont utilisées comme une carte Légende. Si le juge de la manche choisit la carte Hameçonnage au lieu de la carte Légende, il doit remettre une de ses cartes Photo au joueur qui a soumis la carte. Si le juge n'a pas encore obtenu une carte Photo, il perd son tour et est exclu de la manche suivante.

C'est au joueur qui a placé la carte Hameçonnage de dénoncer le juge qui s'est laissé tromper par sa carte. Les autres joueurs peuvent signaler une carte Hameçonnage, mais seul le joueur qui a joué cette carte peut remporter le point. Dès lors, les autres joueurs n'ont aucun intérêt à le faire.

CARTES MALICIELS

Contrairement à la vraie vie, les cartes Maliciel sont clairement identifiées comme telles. Le joueur qui en détient une peut échanger ses cinq cartes Légende contre celles du joueur de son choix. La carte Maliciel est alors mise de côté.

Les cartes Maliciel sont regroupées avec les cartes Légende et pigées de la même façon. Lorsqu'un joueur pige une carte Maliciel, il ne peut la jouer qu'au début d'une manche après que tous les joueurs aient pigé une nouvelle carte Légende, mais avant que le juge n'ait pigé une nouvelle carte Photo. Le joueur qui a perdu une carte doit en piger une nouvelle.

CARTES CYBERSÉCURITÉ

Les cartes Cybersécurité protègent le joueur contre les cartes Hameçonnage et Maliciel. Ces cartes ne sont pas regroupées avec les autres, mais obtenues par le joueur après qu'il ait fait une action précise. Une action différente est rattachée à chaque type de carte Cybersécurité, mais le résultat est le même pour chaque type de carte

Cartes Éducation : Prenez un égoportrait de vous en train de jouer et partagez-la avec #PensezCybersecurite. N'oubliez pas de taguer @PensezCybersecurite!

Cartes Authentification multifactorielle : Activez l'authentification multifactorielle d'un compte ou d'un appareil.

Cartes Mises à jour logicielles : Activez la mise à jour automatique d'un appareil ou d'une application.

Cartes Pensez cybersécurité : Appelez ou envoyez un message texte à une membre de votre famille pour leur souhaiter de joyeuses fêtes (oui… même si vous jouez en juin!).

Les cartes Cybersécurité ne peuvent être obtenues qu'en début de manche et les joueurs peuvent en accumuler un maximum de quatre dans une partie. Lorsqu'une carte Cybersécurité a été jouée, elle ne peut être utilisée de nouveau.