PENSEZ CYBERSÉCURITÉ

TROUSSE POUR LES RÉSEAUX SOCIAUX

Soutenir la campagne Pensez cybersécurité est une chose facile et cette trousse pour les réseaux sociaux rend la chose encore plus simple.

Vous pouvez utiliser les messages inclus dans la trousse pour faire la promotion de la campagne Pensez cybersécurité dans votre entreprise, les organismes sans but lucratif, les communautés scolaires et sur les réseaux privés.

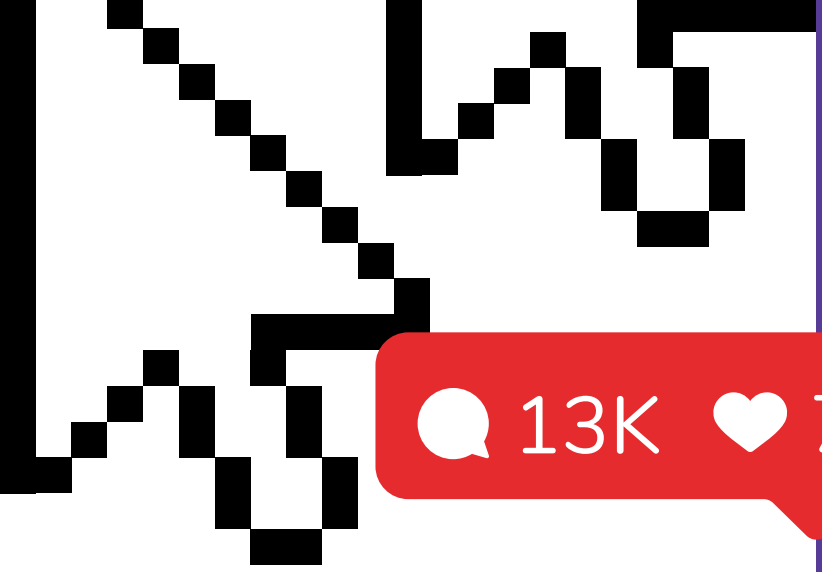
QUE CONTIENT LA TROUSSE ?

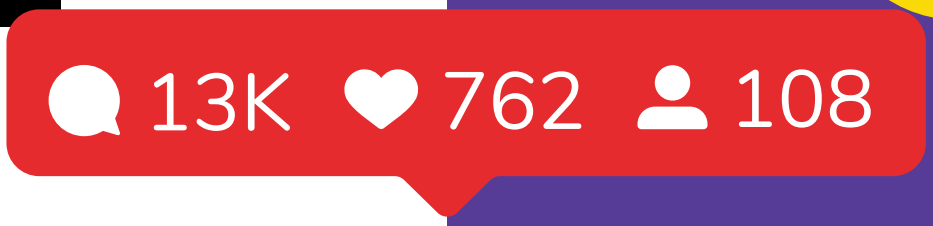
Cette trousse contient tout ce dont vous avez besoin pour être un véritable ambassadeur Pensez cybersécurité. Elle comprend :

- 10 messages à publier sur Facebook, Twitter et LinkedIn
  - 2 messages généraux sur la cybersécurité
  - 2 messages sur l'hameçonnage
  - 2 messages sur l'authentification multifactorielle
  - 2 messages sur la mise à jour logicielle
  - 3 messages sur la création de mots de passe robustes
- Des éléments graphiques à utiliser avec les messages

Centre de la sécurité des télécommunications

Canada





CRÉEZ VOTRE PROPRE CONTENU

À titre de partenaire de Pensez cybersécurité, vous pouvez bien sûr créer vos propres messages. Pour vous aider, nous avons préparé quatre fiches d'information. Vous pouvez également consulter la page Ressources de notre site web où vous trouverez des vidéos, des infographies et d'autres visuels à partager que vous pourrez utiliser sur vos réseaux sociaux.

TÉLÉCHARGER LES FICHES D'INFORMATION

N'oubliez pas d'utiliser le mot-clic #PensezCybersécurité lorsque vous publiez vos messages afin que vos abonnés puissent avoir un complément d'information!

SUIVEZ PENSEZ CYBERSÉCURITÉ SUR LES RÉSEAUX SOCIAUX

Pensez cybersécurité publie fréquemment sur ses comptes de réseaux sociaux des mises à jour sur les plus récents conseils en matière de cybersécurité. Suivez-nous sur Twitter, Facebook, LinkedIn et Instagram pour avoir plus de contenu que vous pourrez partager sur vos réseaux.

@PensezCybersécurité

MESSAGES POUR LES AMBASSADEURS DE PENSEZ CYBERSÉCURITÉ

Ces messages sont conçus pour être publiés sur Facebook, Twitter et LinkedIn. Vous pouvez également les utiliser sur d'autres plateformes si vous le désirez, mais vérifiez bien certaines limites comme le nombre de caractères et adaptez les messages à chaque plateforme au besoin!

GÉNÉRALE

Les technologies évoluent constamment et il peut être difficile de suivre cette évolution. Suivez @Pensezcybersécurité pour connaître les plus récentes recommandations et les conseils des experts en matière de cybersécurité.

Il n'est pas nécessaire d'être un professionnel des TI pour contrer une cyberattaque. @Pensezcybersécurité offre de nombreuses ressources expliquant les étapes simples permettant de se protéger en ligne.

Voici comment vous pouvez penser cybersécurité :
https://www.pensezcybersecurite.gc.ca/fr/devenez-un-ambassadeur

MISES À JOUR LOGICIELLES

Les mises à jour logicielles ne consistent pas à obtenir les plus récents gadgets pour nos appareils. Elles contiennent des dispositifs importants qui vous protégeront (et protégeront vos appareils) contre les cybermenaces.

Suivez @PensezCybersécurité si vous avez besoin d'aide pour télécharger et installer les mises à jour.

Vous ignorez les mises à jour de système sur votre téléphone ou votre ordinateur ?

Bien sûr, il est facile de les ignorer, mais ne pas faire les mises à jour met votre appareil ou votre ordinateur à risque. #PensezCybersécurité et mettez à jour votre système d'exploitation lorsque vous y êtes invité.
https://www.pensezcybersecurite.gc.ca/fr/ressources/mettez-jour-votre-logiciel

HAMEÇONNAGE

Si vous avez une adresse courriel ou un téléphone cellulaire, vous avez probablement déjà reçu un message d'hameçonnage. Vous n'êtes pas seul : l'hameçonnage est aujourd'hui la troisième tentative de fraude en ligne la plus fréquente au Canada.

Protégez-vous en suivant ces conseils de @PensezCybersécurité : www.pensezcybersecurite.gc.ca/fr/ressources/video-hameconnage-ne-mordez-pas

L'hameçonnage est l'une des tentatives de fraude les plus courantes en ligne. Heureusement, les messages d'hameçonnage sont généralement faciles à repérer… si vous savez ce que vous devez surveiller.

Voici quelques-uns des signes que vous devez surveiller : www.pensezcybersecurite.gc.ca/fr/ressources/les-7-signaux-dalarme-de-lhameconnage #PensezCybersécurité

MOTS DE PASSE

Vos mots de passe protègent vos renseignements personnels, votre identité et même votre argent contre les cybercriminels. Assurez-vous qu'ils sont robustes en suivant ces conseils de @PensezCybersécurité : www.pensezcybersecurite.gc.ca/fr/ressources/video-creez-un-mot-de-passe-robuste

Tous les mots de passe ne sont pas créés égaux… Apprenez à créer un mot de passe robuste en suivant ces conseils de @PensezCybersécurité : www.pensezcybersecurite.gc.ca/fr/securisez-vos-comptes/phrases-de-passe-mots-de-passe-et-nip

Les mots de passe robustes, c'est génial, mais les phrases de passe robuste le sont encore plus. Apprenez à créer une phrase de passe robuste pour protéger vos comptes en suivant ces conseils de @PensezCybersécurité : www.pensezcybersecurite.gc.ca/fr/ressources/video-creez-un-mot-de-passe-robuste

AUTHENTIFICATION MULTIFACTORIELLE

Activez l'authentification multifactorielle pour vos comptes importants afin d'assurer la cybersécurité de vos renseignements personnels. Cela peut sembler compliqué, mais ça ne l'est pas. En fait, vous utilisez tous les jours l'authentification multifactorielle!

Pour en savoir plus : www.pensezcybersecurite.gc.ca/fr/ressources/video-lauthentification-multifactorielle #PensezCybersécurité

Qu'est-ce que l'authentification multifactorielle ?

L'authentification multifactorielle consiste à avoir deux mesures de sécurité pour pouvoir accéder à un appareil ou à un compte. Pour activer dès aujourd'hui l'authentification multifactorielle, suivez ces conseils de @PensezCybersécurité : www.pensezcybersecurite.gc.ca/fr/securisez-vos-comptes/authentification-multifactorielle