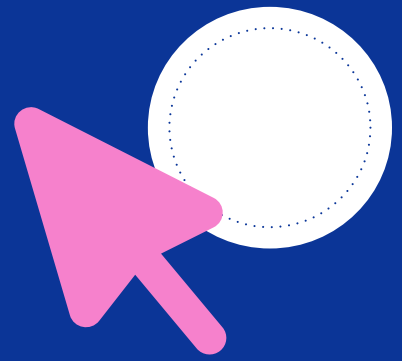
VOTRE GUIDE DU

MOIS DE LA SENSIBILISATION À LA CYBERSÉCURITÉ 2020



PENSEZCYBERSECURITE.CA

Canada

QU’EST-CE QUE PENSEZ CYBERSÉCURITÉ?

Pensez cybersécurité est une campagne du Centre de la sécurité des télécommunications du gouvernement du Canada qui a pour but d’informer les Canadiens sur les moyens d’assurer facilement leur sécurité en ligne.

QU'EST-CE QUE LE MOIS DE LA SENSIBILISATION À LA CYBERSÉCURITÉ?

Le Mois de la sensibilisation à la cybersécurité (MSC) est une campagne internationale qui a lieu au mois d'octobre de chaque année pour sensibiliser le public à l'importance de la cybersécurité.

Cette année, le MSC vous propose de vous lier d'amitié avec vos appareils, une façon de reconnaître tout ce qu'ils font pour nous simplifier la vie. Chaque semaine, un type d'appareils sera en vedette et nous traiterons des façons d'assurer leur cybersécurité.

SEMAINE 1: FAIRE LE POINT

1 AU 3 OCTOBRE

Les appareils intelligents font maintenant partie de nos vies quotidiennes, à tel point qu'il est facile de perdre le compte de tous les appareils que nous possédons. Pour débuter ce MSC, il convient donc de faire le point et notamment de se débarrasser des appareils qui nous ont rendus de fiers services, certes, mais que nous n'utilisons plus.

SEMAINE 2:
SEMAINE DU TÉLÉPHONE
4 AU 10 OCTOBRE

Que ce soit pour communiquer avec vos proches, terminer un travail pour le bureau ou simplement passer le temps, votre téléphone vous accompagne dans toutes vos activités quotidiennes. Bien en prendre soin est la moindre des choses et la meilleure façon de le faire est de vous assurer qu'il est bien protégé.

Cette semaine, suivez ces conseils pour pouvoir utiliser votre téléphone en toute cybersécurité:

- **Faites les mises à jour logicielles**
- **Surveillez l'hameçonnage**
- **Activez l'authentification multifactorielle**

MISES À JOUR LOGICIELLES ET DU SYSTÈME D'EXPLOITATION

Faire les mises à jour logicielles n'est peut-être pas très agréable, mais c'est la façon la plus simple de protéger nos appareils. De plus, elles vous donnent accès à de nouvelles fonctionnalités et corrigent des bogues qui en améliorent le fonctionnement.

Activez la mise à jour automatique chaque fois que cela est possible pour protéger parfaitement votre téléphone!

En savoir plus sur les mises à jour

- Mises à jour système
- Votre logiciel fait très… 2019
- Vidéo: mises à jour logicielles

Des Canadiens ont activé les mises à jour automatiques

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité, EKOS Research Associates Inc., 2020

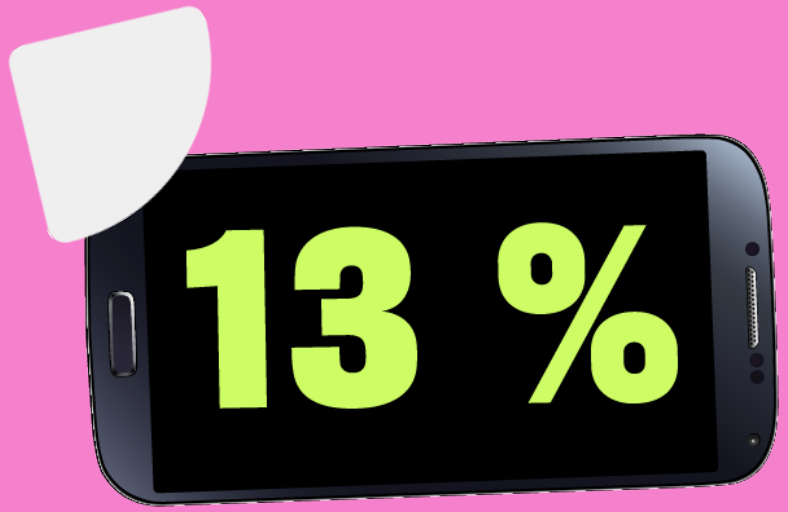
HAMEÇONNAGE PAR MESSAGE TEXTE

Les attaques d'hameçonnage par message texte sont des messages frauduleux qui prétendent provenir d'une source légitime dans le but de vous amener à dévoiler vos renseignements personnels ou de voler votre argent.

N'envoyez jamais de renseignements personnels par texto si vous n'êtes pas absolument certain de l'identité de l'expéditeur.

En savoir plus sur l'hameçonnage par message texte

- Les 7 signaux d'alarme de l'hameçonnage
- Urgent: votre mot de passe a été réinitialisé avec succès
- Hameçonnage: ne mordez pas à l'hameçon!



Des Canadiens ont été victimes d'hameçonnage par message texte sur leur téléphone

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité, EKOS Research Associates Inc., 2020

AUTHENTIFICATION MULTIFACTORIELLE

L'authentification multifactorielle offre une barrière de sécurité additionnelle, car elle exige deux preuves d'identité avant d'autoriser l'accès à un compte ou un appareil.

Il existe trois types de facteurs d'authentification:

- Ce que vous savez, comme un mot de passe
- Ce que vous possédez, comme une clé USB
- Ce que vous êtes, comme vos empreintes digitales

En savoir plus sur l'authentification multifactorielle

- L'authentification multifactorielle
- Avec l'authentification multifactorielle, la cybersécurité est une affaire personnelle!
- Vidéo: l'authentification multifactorielle

Proportion de Canadiens qui utilisent l'authentification multifactorielle

Sondage auprès d'utilisateurs d'Internet sur la cybersécurité, Santé publique Canada, 2018

SEMAINE 3:
SEMAINE DE L'ORDINATEUR
11 AU 17 OCTOBRE

Les téléphones, c'est génial, mais ils ne peuvent faire certaines choses aussi bien que nos bons vieux ordinateurs de bureau ou portables, comme jouer en ligne, répondre aux courriels ou rédiger un document pour le travail. Montrons-leur notre appréciation en prenant le plus grand soin.

Cette semaine, nous discutons de ce que vous pouvez faire pour protéger votre ordinateur:

- **Phrases et mots de passe complexes**
- **Protection contre les maliciels**
- **Attaques par hameçonnage**

PHRASES ET MOTS DE PASSE

Un mot de passe robuste peut faire toute la différence lorsqu'il est question de protéger nos comptes et appareils. De façon générale, un mot de passe robuste:

- Comporte entre 8 et 12 caractères
- Comprend des lettres minuscules et majuscules, des chiffres et des symboles
- Ne contient aucun renseignement personnel

Et pour une sécurité encore meilleure, utilisez plutôt une phrase de passe, soit un série de 4 mots choisis au hasard et comprenant au moins 15 caractères.

Proportion de Canadiens qui modifient leurs mots de passe au moins à quelques reprises chaque année

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité, EKOS Reearch Associates Inc., 2020

MALICIEL

Un maliciel est un logiciel malveillant qui infecte les ordinateurs et permet aux cybercriminels de les infiltrer ou de les endommager.

Vous pouvez éviter les maliciels en ne cliquant pas sur des liens suspects, en ne téléchargeant que les fichiers provenant de sources sûres et en faisant les mises à jour de votre logiciel antivirus.

En savoir plus sur les maliciels

- Maliciel détecté!
- Ce qu'est un maliciel: comment se protéger
- Vidéo: Maliciels et rançongiciels

Proportion de Canadiens dont l'ordinateur a été infecté par un maliciel

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité, EKOS Reearch Associates Inc., 2020

HAMEÇONNAGE

Comme l’hameçonnage par message texte, l’hameçonnage consiste à prétendre représenter une organisation légitime ou une personne que vous connaissez dans le but de vous voler vos renseignements personnels ou votre argent.

Les attaques par hameçonnage sont souvent difficiles à détecter, mais vous pouvez vous en protéger en en reconnaissant les signes.

En savoir plus sur les tentatives d’hameçonnage

- Pourquoi les cyberfraudes réussissent-elles à nous piéger?
- Trois fraudes par hameçonnage courantes
- Les indices de l’hameçonnage: comment vous protéger

Proportion de Canadiens qui disent avoir répondu sans le savoir à un message d’hameçonnage

Sondage auprès d’utilisateurs d’Internet sur la cybersécurité, Santé publique Canada, 2018

SEMAINE 4:
SEMAINE DES RÉSEAUX
DU 18 AU 24 OCTOBRE

Une évidence: personne ne se place en file au petit matin pour se procurer le plus récent routeur. Après tout, ils sont moins élégants que nos téléphones ou nos ordinateurs, mais ils jouent un rôle important: ils nous branchent au reste du monde. Alors traitons ces héros silencieux comme ils le méritent et protégeons-les!.

Cette semaine, vous saurez tout sur:

- **La configuration d'un réseau Wi-Fi sécurisé**
- **L'utilisation sécuritaire du Wi-Fi**
- **La protection de votre réseau Wi-Fi d'entreprise**

Pour souligner la semaine de la PME, nous offrons des conseils de cybersécurité aux petites et moyennes entreprises.

CONFIGURER UN RÉSEAU SÉCURISÉ

Votre réseau Wi-Fi connecte tous vos appareils les uns aux autres, et si jamais il est compromis, tous vos appareils sont à risque.

Assurez-vous de créer un mot de passe complexe et unique pour accéder à votre routeur et pensez à créer un réseau pour vos invités afin d'éviter que des inconnus n'accèdent à votre réseau principal.

En savoir plus sur les réseaux Wi-Fi privés

- Les réseaux privés
- Trois façons d'assurer notre cybersécurité (lorsqu'on travaille de la maison)
- COVID-19: Comment configurer un réseau sécurisé pour le travail à la maison en pleine pandémie

Des Canadiens n'utilisent pas le mot de passe par défaut de leur routeur

Sondage de suivi sur la campagne Pensez cybersécurité, EKOS Research Associates Inc., 2020

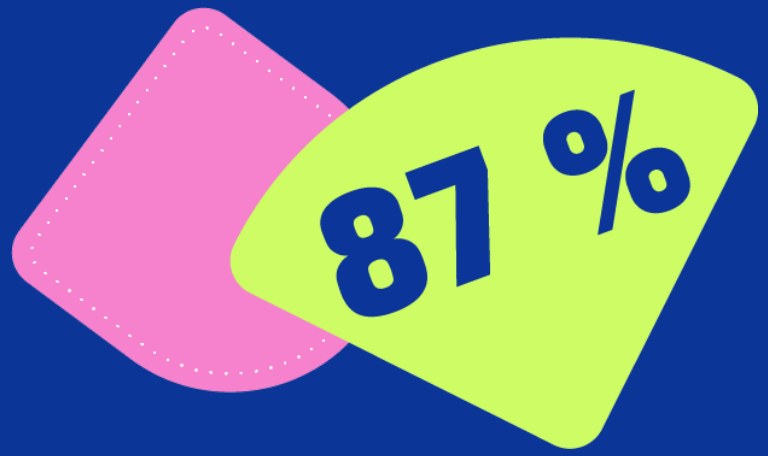
UTILISER LE WI-FI EN TOUTE SÉCURITÉ

Si vous n’êtes pas vigilant, les réseaux Wi-Fi que vous utilisez, surtout s’ils sont publics, peuvent vous rendre vulnérables aux cyberattaques.

Si vous utilisez un réseau Wi-Fi public, évitez de vous connecter à un compte ou vous stockez des renseignements personnels et, si possible, utilisez un RPV.

En savoir plus sur la connexion en toute sécurité

- Réseaux Wi-Fi publics
- RPV



Des consommateurs mettent leurs renseignement personnels à risque lorsqu’ils utilisent un réseau Wi-Fi public

Rapport sur les risques du Wi-Fi 2017, Norton par Symantec, 2017

PROTÉGER VOTRE ENTREPRISE

Les cybercriminels ne ciblent pas uniquement les personnes: elles visent aussi les entreprises. Ces dernières sont souvent victimes d'hameçonnage, de maliciels et autres cybermenaces.

Pour se protéger, elles doivent se doter d'un plan en matière de cybersécurité que devront suivre leurs employés et qui comprendra des règles sur l'utilisation des réseaux sociaux et de la messagerie électronique.

En savoir plus sur la cybersécurité des entreprises

- Comment développer un plan de cybersécurité pour l'entreprise
- Cybersécurité et commerce en ligne: une introduction
- Cybersécurité des PME: pourquoi les mises à jour logicielles sont essentielles

SEMAINE 5:
SEMAINE DES APPAREILS INTELLIGENTS
25 au 31 octobre

Si votre ordinateur était il y a longtemps votre meilleur ami, ce statut appartient peut être maintenant à vos appareils intelligents... Un peu bizarre, peut-être, mais bientôt, vous vous demanderez comment vous avez pu vivre sans lui!

Au programme cette semaine, comment prendre soin de votre télé, de votre carillon et de vos autres appareils intelligents:

- **Configurer le réseau Wi-Fi pour vos appareils intelligents**
- **Modifier vos paramètres de confidentialité**
- **L'Internet des objets à la maison et dans les entreprises**

CONFIGURER LE RÉSEAU WI-FI POUR VOS APPAREILS INTELLIGENTS

Vos appareils intelligents contiennent beaucoup de renseignements sur vous, comme votre horaire, les renseignements de votre carte de crédit et bien plus encore.

Pour éviter que ces renseignements se retrouvent entre les mains de gens mal intentionnés, créez un réseau secondaire réservé à vos appareils intelligents. Ainsi, votre réseau Wi-Fi principal et les appareils qui y sont connectés seront protégés.

En savoir plus sur les façons de protéger nos appareils intelligents

- Télés et autres appareils intelligents
- Réseaux privés

des Canadiens utilisent un réseau invités pour leurs visiteurs et leurs appareils intelligents

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité, EKOS Research Associates Inc., 2020

PROTÉGER VOS APPAREILS INTELLIGENTS

Aussi intelligents soient-ils, nos appareils intelligents ont toujours besoin de nous pour les protéger.

Heureusement, ce n’est pas bien compliqué: les mêmes mesures que pour notre téléphone, notre ordinateur et notre tablette s’appliquent (comme l’authentification multifactorielle, les mises à jour logicielles et les mots de passe robustes).

En savoir plus sur la confidentialité des appareils intelligents

- L’authentification multifactorielle
- Les mises à jour logicielles
- Les mots et phrases de passe

des Canadiens ont fait des recherches pour savoir comment protéger leurs appareils intelligents

Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité, EKOS Research Associates Inc., 2020

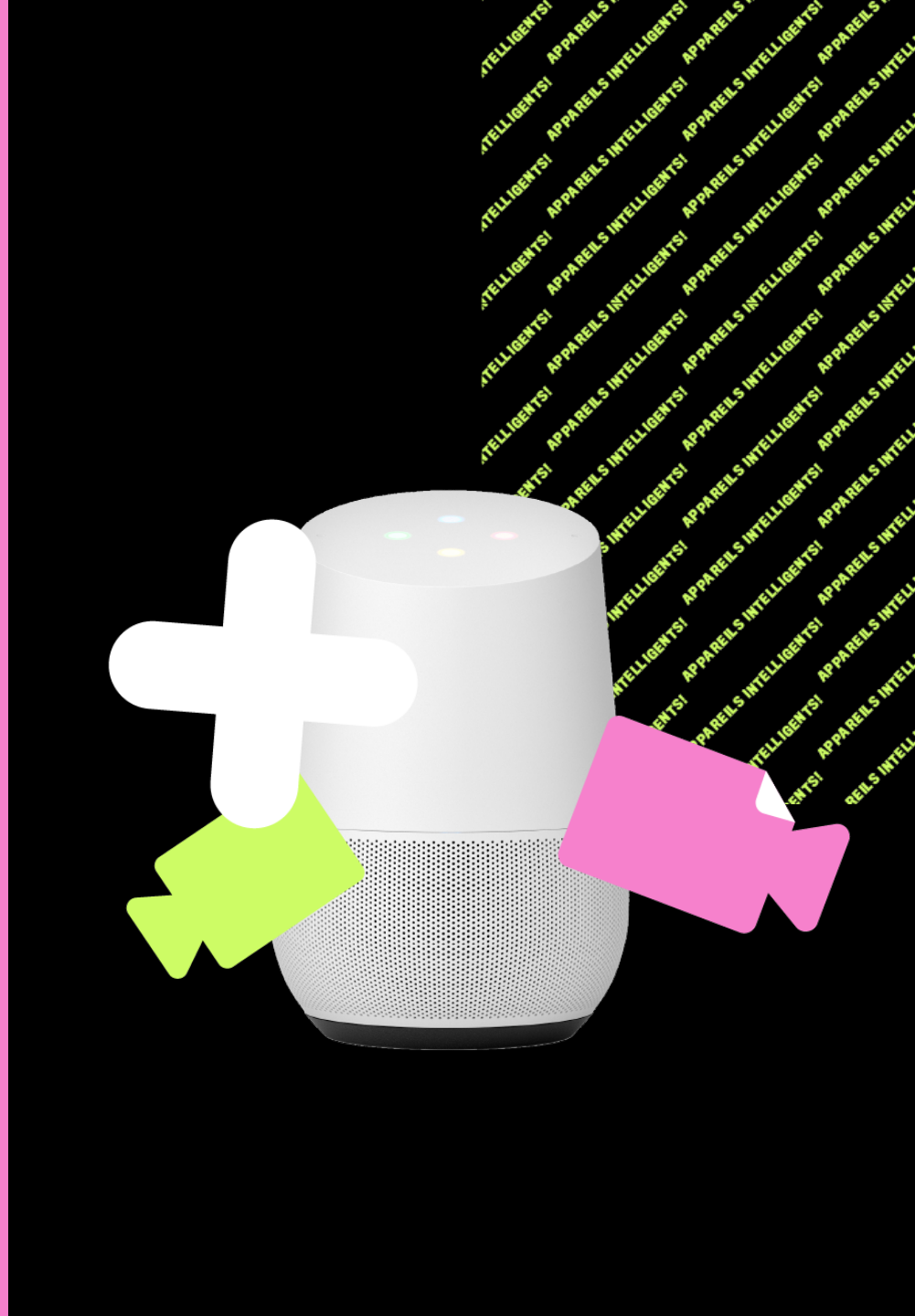
LES ENTREPRISES ET L'INTERNET DES OBJETS

L'Internet des objets est un autre terme pour designer les appareils intelligents. Il regroupe une grande variété d'objets comme des assistants vocaux, haut-parleurs pour gérer votre horaire, de nombreux outils dont ont besoin les diverses industries, etc.

Malheureusement, comme pour tout ce qui est connecté à l'Internet, les appareils intelligents peuvent être la cible de cybercriminels et les entreprises doivent donc mettre en œuvre un plan pour les protéger.

En savoir plus sur l'Internet des objets

- La trousse Internet des objets pour les PME
- L'Internet des objets et la sécurité
- PowerPoint: L'Internet des objets



D’AUTRES RESSOURCES POUR LE MSC

Vous voulez tout savoir sur les façons de protéger vos appareils? Consultez les ressources que nous avons conçues pour le MSC, y compris nos guides, nos listes de vérification et plus encore!

- Vidéos de la campagne
- Fiches d’information
- Blogues hebdomadaires
- Affiche pour les PME

VOUS VOULEZ VOUS ENGAGER?

Plus les Canadiens sauront comment se protéger en ligne, mieux ce sera pour nous tous. Et la meilleure façon de le faire, c’est que chacun de nous s’engage!

Nous pouvons tous participer au Mois de la sensibilisation à la cybersécurité. Et nous vous facilitons la chose! Tout ce que vous avez à faire, c’est de consulter nos ressources et de les partager.

- Trousse pour les réseaux sociaux
- Fiches d’information
- Bannières Web
- Fonds d’écran pour appels vidéos

SUIVEZ-NOUS SUR LES RÉSEAUX SOCIAUX POUR D'AUTRES CONTENUS À PARTAGER

Twitter

Facebook

Instagram

LinkedIn

QUESTIONS OU COMMENTAIRES?

Rejoignez Pensez cybersécurité en communiquant avec le Centre canadien pour la cybersécurité:

- Courriel: contact@cyber.gc.ca
- Sans frais: 1-833-CYBER-88 (1-833-292-3788)

MERCI D'AIDER LES CANADIENS ET PENSEZ CYBERSÉCURITÉ!

MOIS DE LA SENSIBILISATION À LA CYBERSÉCURITÉ

METTEZ VOS APPAREILS À JOUR

PENSEZCYBERSECURITE.CA

Canada