CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

CANARIE

Webinaire mensuel sur la Cybersécurité

Cyber Centre et ses services

Janvier 2021

Les réseaux canadiens et les renseignements personnels des Canadiens doivent être protégés contre les adversaires.

La protection de ces systèmes, ce n'est pas une question simple d'efficacité opérationnelle; c'est aussi une question de sécurité nationale, de défense de la souveraineté et de protection de la vie privée.

Le rôle du CST en cybersécurité

- AUTORITÉ CANADIENNE EN MATIÉRE DE CYBERSECURITÉ
- ACCÈS À DES RENSEIGNEMENTS ÉTRANGERS UNIQUES
- AVANT LES MENACES ÉMERGENTES
- SURVEILLANCE DES SYSTEMES GC 24/7 – CYBER MENACES
- PROTEGE LES INFORMATIONS CANADIENNES LES PLUS IMPORTANTES

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Sécurité des technologies de l'information (CST) + Centre des operations de sécurité (Services partagés Canada) + Centre canadien de réponse aux incidents cybernétiques (Sécurité Publique) = Centre canadien pour la cybersécurité

Augmentation de la portée des services de cybersécurité

Loi sur la défense nationale

Le CST peut fournir des conseils, des orientations et des services pour protéger les infrastructures d'information importantes pour le GC.

Loi sur le CST

En août 2019 - Le CSE est désormais autorisé à fournir des services de cyberdéfense plus robustes en déployant ses outils de cyberdéfense pour les réseaux non gouvernementaux critiques désignés comme étant d'importance pour le Canada.

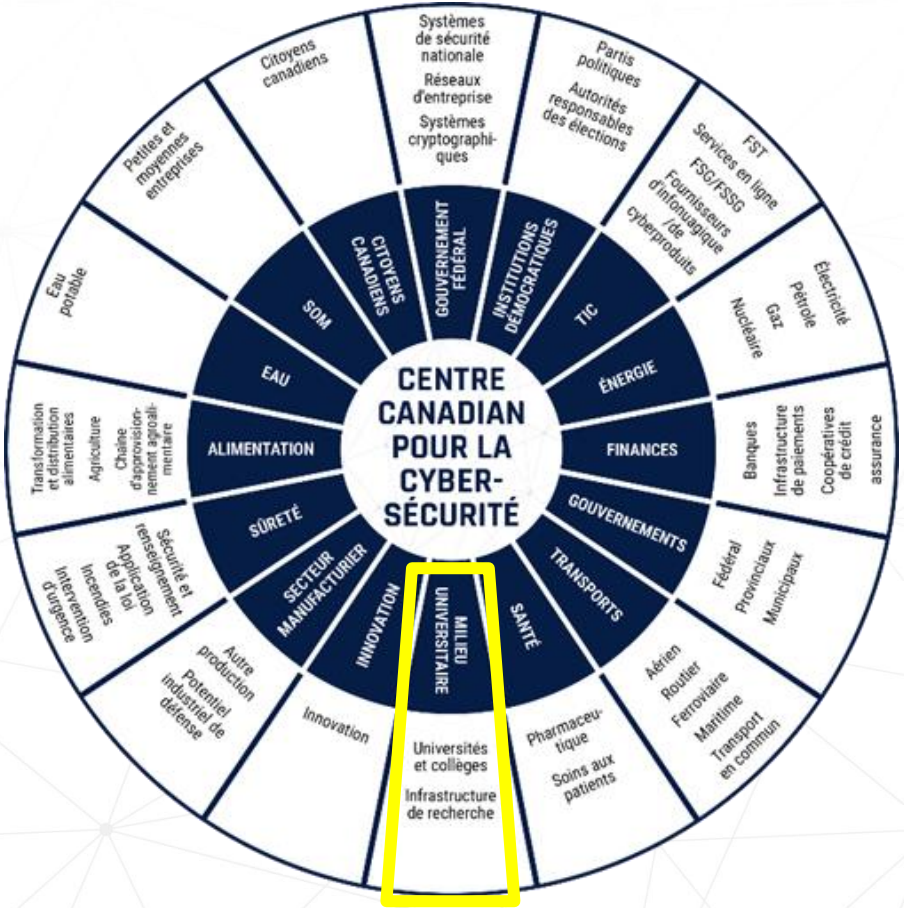
LA CYBER SÉCURITÉ ET L'ASSURANCE DE L'INFORMATION

DÉFENDRE D'IMPORTANTS RÉSEAUX NON GOUVERNEMENTAUX DU CANADA

Sur demande, déployez les outils de cybersécurité du CST sur des systèmes non gouvernementaux.

Supprimer les obstacles juridiques au partage d'informations sur les cybermenaces et de conseils d'atténuation.

Secteurs d'engagement en matière de cybersécurité



À qui s'adressent nos services?

Nous accueillons les partenariats visant à créer un cyberespace canadien fort et résilient. Nous offrons des espaces polyvalents et non classifiés que peuvent employer conjointement le gouvernement, l'industrie privée et le milieu universitaire.

Gouvernement

- Nous sommes une ressource centralisée qui agit à titre d'interlocuteur pour les hauts dirigeants du gouvernement pour tout ce qui touche à la cybersécurité.

Partenaires externes

- Nous représentons le point de contact principal du gouvernement fédéral en matière de cybersécurité pour les partenaires externes, notamment dans le cadre de la coordination et de l'intervention en cas d'incident.

Application de la loi

- Nous sommes la seule source autorisée à fournir de l'expertise technique en matière de cybersécurité qui vient appuyer les organismes responsables dans le cadre de leurs fonctions policières et de leurs activités de sécurité et de renseignement.

Canadiens

- Nous informons et sensibilisons les Canadiens sur les enjeux de cybersécurité, et nous communiquons avec eux à ce sujet, en leur fournissant des conseils clairs et des pratiques qui sont appuyés par une expertise et des renseignements uniques.

Vision et mission du Centre canadien pour la cybersécurité

VISION - *NOTRE BUT*

UN CANADA NUMÉRIQUE SÉCURITAIRE

MISSION - *NOTRE PROMESSE*

PROTÉGER
Protéger le Canada grâce à des capacités avancées en cybersécurité.

INFORMER
Fournir aux Canadiens des avis et des conseils fiables et officiels en matière de cybersécurité.

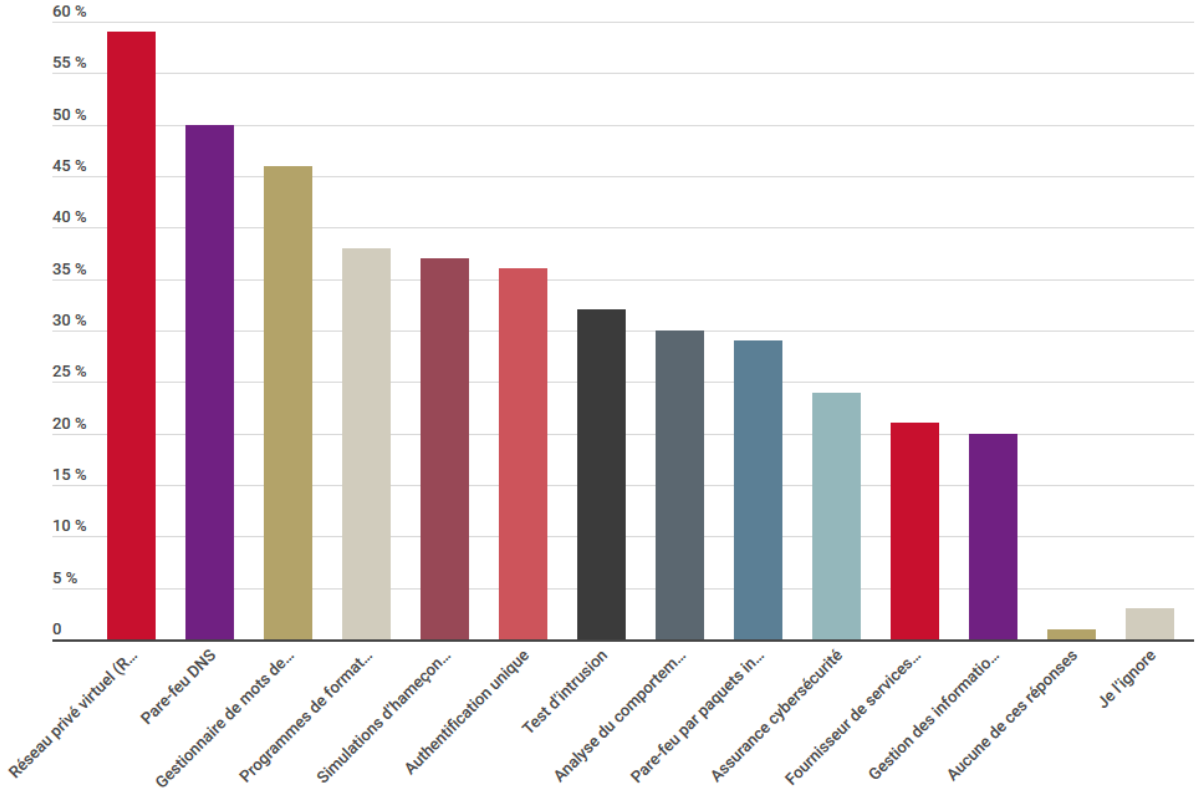
DYNAMISER
Renforcer la cybersécurité du Canada grâce à la collaboration, à l'innovation et aux partenariats.

ÉVALUATION DES CYBERMENACES NATIONALES 2020

- Le nombre de **cyberattaques** augmente et devient de plus en plus sophistiqué.
- La **cybercriminalité** et les **rançongiciels** continueront de cibler les secteurs d'infrastructure critique.
- Les programmes parrainés par les États-nation de la Chine, de la Russie, de l'Iran et de la Corée du Nord représentent la plus grande menace stratégique pour le Canada alors qu'ils mènent de **l'espionage** contre les entreprises, le secteur **académiques** et le gouvernement canadien pour voler la propriété intellectuelle canadienne.

Rapport sur la cybersécurité de 2020 de l'ACEI (2020)

Lequel des types de couches de cybersécurité suivants, le cas échéant, votre organisation déploie-t-elle pour répondre à l'augmentation des cybermenaces mondiales?



Reference :
https://www.cira.ca/fr/cybersecurity-report-2020

Les cyberattaques par an (2020)

80% POURCENTAGE D'ORGANISATIONS QUI ONT FAIT FACE À UNE CYBER-ATTAQUE AU COURS DE LA DERNIÈRE ANNÉE

21% POURCENTAGE DES ORGANISATIONS QUI ONT FAIT FACE à PLUS DE 10 ATTAQUES AU COURS DE LA DERNIÈRE ANNÉE

Reference : https://www.cira.ca/fr/cybersecurity-report-2020

Politique de mise à jour (2020)

Votre organisation maintient-elle une politique formelle d'application de correctifs?

Reference : https://www.cira.ca/fr/cybersecurity-report-2020

Nos services

1. Appels communautaire du secteur
2. Outil canadian de cybersecurity (OCC)
3. Sessions de formation et de sensibilisation
4. Notifications de cybermenaces
5. Outils de cyberdéfense personnalisés

1. APPEL COMMUNAUTAIRE DU SECTEUR ACADÉMIQUE

Le but est de partager l'expertise cybernétique pertinente du secteur

- Construire une communauté de confiance
- Fournir une connaissance situationnelle
- Offert à cadence régulière
  (bihebdomadaire, débutant en février 2021)

Pour recevoir l'invitation, envoyer votre demande à

marie-claude.belanger@cyber.gc.ca

2. Outil canadien de cybersécurité (OCC)

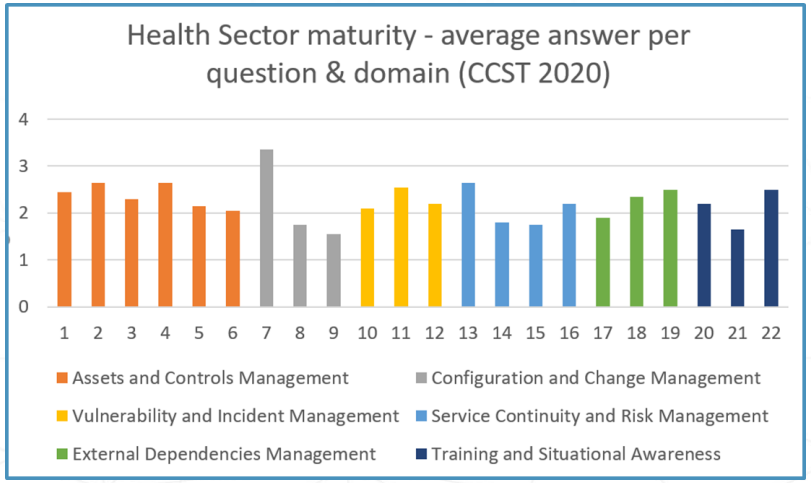
- Qu'est-ce que c'est?
  - Outil d'auto-évaluation en ligne conçu pour être complété en moins de 60 minutes.
  - Pertinent pour les entités avec un large éventail de postures cyber
- Quel est son but?
  - Pour mieux comprendre le risque auqeul vous faites face afin de mieux servir l'établissemetn avec des conseils, des services et un soutien appropriés.
- Quels sont les rapports de l'outil?
  - Des conseils personnalisés sont fourni, scores spécifiques à l'entité et une comparaisons au secteur.

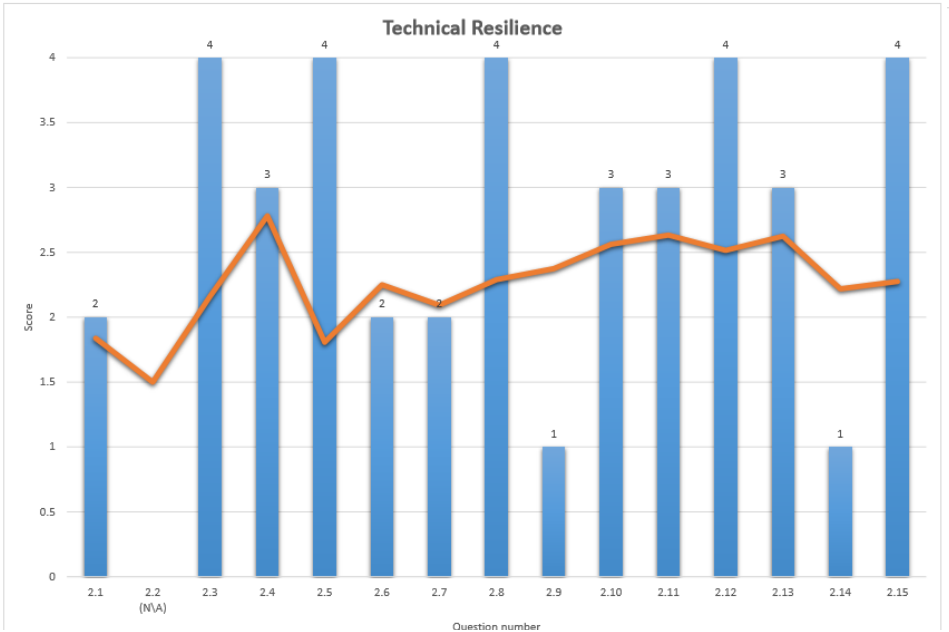
Demander votre demande d'accès à marie-claude.belanger@cyber.gc.ca

Canadian Cyber Security Tool

BUILDING A SAFE AND RESILIENT CANADA

Résultats du programme et de la resilience technique





Outil Canadien de cybersécurité | Canadian Cyber Security Tool

BÂTIR UN **CANADA SÉCURITAIRE** ET **RÉSILIENT** | BUILDING A **SAFE** AND **RESILIENT CANADA**

3. Formation et session de sensibilization : Carrefour de l'apprentissage

- Vidéos réenregistrées (3 heures)
  - 107 — La cybersécurité dans le GC pour les employés non-TI
  - 110 — La cybersécurité dans le GC et la visibilité en ligne
  - 111 — La cybersécurité dans le GC pour les réseaux domestiques et le télétravail
- Apprentissage en ligne (30-60 min)
  - 602 – Découvrir la cybersécurité
- Mini-sessions en direct (90 min)
  - 151 – Prévention de la cybercriminalité
  - 152 – Protection des renseignemetns personnels numérique
  - 153 – Cybersécurité et le télétravail
  - 154 – Cybersécurité relative à l'Internet des objects
  - 155 – Renforcer l'authentification

https://cyber.gc.ca/fr/carrefour-de-lapprentissage
Pour toutes questions, communiquez avec
education@cyber.gc.ca

4. Abonnez-vous aux notifications de cybermenaces

ALERTES
Avis proactifs sur les nouvelles cybermenaces

ALERTES | **Bulletin de sécurité Cisco**

Numéro : AV21-025
Date : 14 janvier 2021

Le 13 janvier 2021, Cisco a publié un bulletin de sécurité visant à corriger une vulnérabilité liée au produit suivant :

- Cisco AnyConnect Secure Mobility Client for Windows – versions antérieures à la version 4.9.04043.

Un auteur de menace pourrait exploiter cette vulnérabilité pour exécuter du code arbitraire sur la machine touchée avec des privilèges SYSTEM.

Le Centre pour la cybersécurité recommande aux utilisateurs et aux administrateurs de consulter les pages Web suivantes et d'appliquer les mises à jour nécessaires :

Cisco AnyConnect
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-injec-pQnryXLf (en anglais seulement)

Site Web du Centre pour la cybersécurité

https://www.cyber.gc.ca/fr/alertes-et-avis

Alertes par courriel

CYBERFLASH
Avis urgents sur des problèmes de sécurité en cours

*De **l'information exploitable** qui décrit **un problème de sécurité immédiat** ou **en cours** qui viserait le gouvernement du Canada ou les systèmes d'importance pour ce dernier.*

```
TITRE
-----
Vulnérabilité liée à la platforme X …

RÉSUMÉ
-------
Le Centre pour la cybersécurité a appris …

DÉTAILS
-------

ACTIONS SUGGÉRÉES
-----------------

INDICATEURS DE COMPROMISSION
------------------------
```

via courriel seulement

Exigences

- Accepter les modalités d'utilisation.
- Fournir les coordonnées de la personne qui recevra et utilisera les avis.

RAPPORTS TECHNIQUES HEBDOMADAIRE

Rapports sur les activities et incidents

Le Rapport technique hebdomadaire propose un résumé technique des activités, des incidents, des produits diffuses par le CCC et des indicateurs de compromission (IC).

via courriel seulement

Exigences

- Accepter les modalités d'utilisation.
- Fournir les coordonnées de la personne qui recevra et utilisera les avis.

5. Outils de cyberdéfense sur mesure

AVIS NCTNS

Cybermenaces détectées dans votre espace adresse IP

*L'avis vous est envoyé lorsqu'un **indicateur de compromis** ou d'un service vulnérable est détecté sur **dans votre espace adresse IP** afin de signaler plus rapidement les cybermenaces et **mieux protéger votre organisation**.*

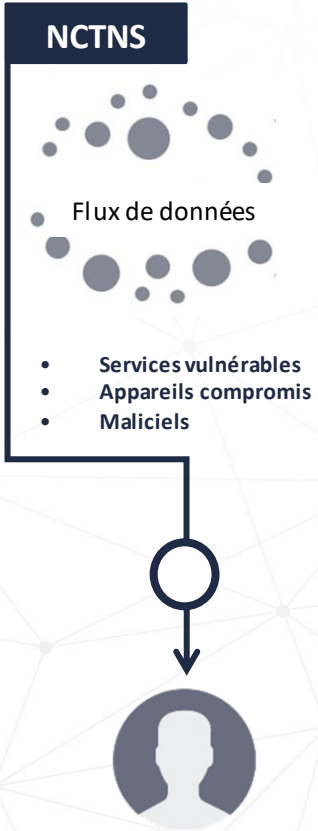
- Données approuvées pour garantir la qualité et un faible taux de faux positifs

Avis par courriel

API
(En développement)

Exigences

- Accepter les modalités d'utilisation.
- Fournir les coordonnées de la personne qui recevra et utilisera les avis.
- Faire part de la plage d'adresses IP propre à votre organisation.



AVENTAIL

Partage d'indicateurs de compromission en temps réel

Partager des indicateurs de compromsission (IC) validés et uniques de façon automatisée

Exigences

- Accepter les conditions d'utilisation et signer une entente de non-divulgation
- Pouvoir deployer une liste blanche d'IPs

Autres services et produits

ANALYSE DE MALICIELS

Soumettez des maliciels pour analyse spécialisée de nos experts

Les Analystes de maliciels et systèmes automatisés du Cyber Centre évaluent et déterminent si les fichiers ou indicateurs de compromission sont malicieux ou non.

Résultats envoyés par courriel

ENVOYER CE QUI SEMBLE SUSPECT

FICHIER SUSPECT

↓

malware@ccirc.ca

PAS UN FICHER

(Indicateurs de compromis, phishing, etc.)

↓

cyberincident@cyber.gc.ca

Règles d'engagement

- Fichiers seront détonés sur l'Internet
- A moins d'avis contraire, les Indicateurs de Compromission seront partagés avec la Communauté de façon anonyme
- Les fichiers doivent être non classifiés (rien de Protégé B ou Classifiés)

FICHE DE POINTAGE

Information exploitable sur les cyber événements

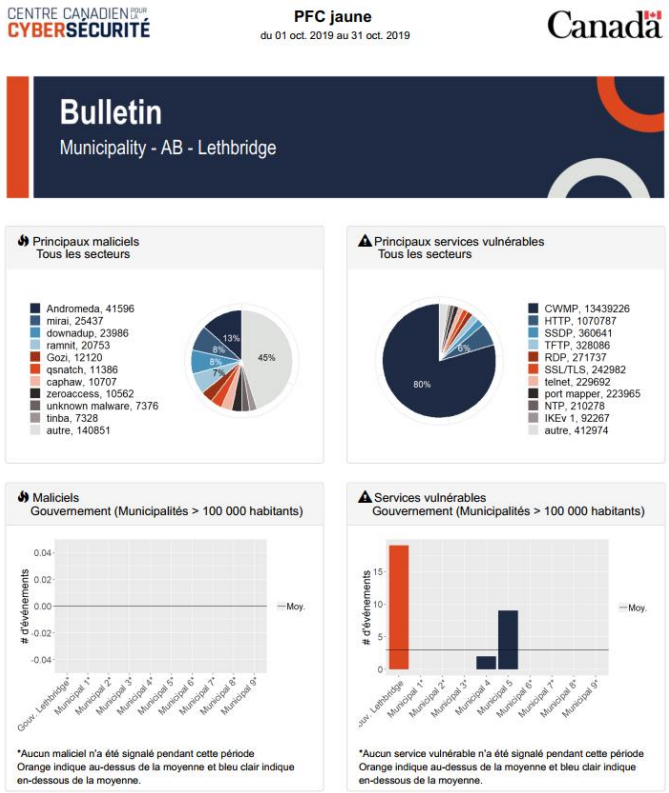
Rapport sur les infections éventuelles, avis de services vulnérables, ***données sur la connaissance de la situation****, et* ***comparaison à d'autres organisations homologues*** *du même secteur.*

Rapports PDF envoyés par courriel tous les mois

(Données brutes CSV disponibles sur demande)

Exigences

- Accepter les modalités d'utilisation.
- Fournir les coordonnées de la personne qui recevra et utilisera les fiches de pointage.
- Faire part de la plage d'adresses IP propre à votre organisation.



Publications

VISITEZ: cyber.gc.ca
sous 'information et conseils'
pour accéder à toutes nos publications

Cyber menaces

- Évaluation des cybermenaces nationales 2020
- Bulletin sur les cybermenaces : Incidence de la COVID-19 sur les activités cybermenaces

Implementing Cyber Security

- Contrôles de cybersécurité de base pour les petites et moyennes organisations
- Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur
- Pratiques exemplaires en matière de cybersécurité : Passation de marché avec des fournisseurs de services gérés
- Rançongiciels : comment les prévenir et s'en remettre
- Protéger l'organisme contre les maliciels
- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage

COVID-19 Related

- Conseils ciblés sur la cybersécurité non classifié applicables durant la pandémie de COVID-19
- Pratiques exemplaires en cybersécurité pour la COVID-19
- Conseils de sécurité pour les organisations dont les employés travaillent à distance

QUI CONTACTER ET QUAND

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ → Signaler des cyber-incidents

cybertip!ca® → Exploitation des enfants, trafic de pornographie enfantine, extorsion d'enfants, etc.

Royal Canadian Mounted Police / Gendarmerie royale du Canada → Cybercriminalité: rancongiciels, blanchiment d'argent, vol d'identité, cyberintimidation, etc.

Centre antifraude du Canada → Si vous recevez un courriel personnel de phishing, du télémarketing, une escroquerie fiscale, etc.

RESTEZ EN CONTACT AVEC NOUS

@CST_CSE
contact@cyber.gc.ca
www.cyber.gc.ca
@cybercentre_ca

Publications du Cyber Centre:
https://cyber.gc.ca/fr/publications

Alertes & Avis du Cyber Centre:
https://cyber.gc.ca/fr/alertes-et-avis

Pour signaler une fraude :
Centre antifraude du Canada
1-888-495-8501
www.antifraudcentre-centreantifraude.ca

Pour signaler un cybercrime :
Service de police local ou
Gendarmerie royale du Canada
www.rcmp-grc.gc.ca

Pour signaler un cyber incident
Centre canadien pour la cybersécurité
contact@cyber.gc.ca