Protéger la démocratie

Trousse d'outils pour résister à LA DÉSINFORMATION et L'INGÉRENCE ÉTRANGÈRE pour les dirigeants communautaires

Désinformation

Fausses informations qui visent délibérément à induire en erreur.

L'ingérence étrangère

Activités délibérées et clandestines de groupes, d'acteurs étatiques ou d'individus qui visent à promouvoir leurs intérêts, souvent en nuisant aux intérêts nationaux du Canada.

La meilleure façon de lutter contre la désinformation et l'ingérence étrangère est de renforcer la résilience par une meilleure connaissance et compréhension de la situation.

Au Canada et dans le monde entier, la démocratie et les institutions démocratiques (p. ex. le Parlement, les assemblées législatives provinciales, le processus électoral) sont depuis longtemps menacées par des personnes ou des groupes dont l'objectif est de les affaiblir et de miner la confiance des citoyens envers le gouvernement.

Cela comprend la désinformation, soit la communication délibérée d'informations inexactes, et l'ingérence étrangère. Ces activités ont un effet négatif sur les personnes vivant au Canada et sur l'unité du pays.

Vous pouvez vous protéger et protéger les autres en prenant conscience des menaces de la désinformation et de l'ingérence étrangère, en apprenant à déceler les fausses informations et en comprenant comment l'information est communiquée et consommée en ligne.

Pour plus d'informations et de ressources, visitez canada.ca/proteger-institutions-démocratiques et securitepublique.gc.ca.

DÉSINFORMATION

Conseils afin de distinguer les faits des fausses informations

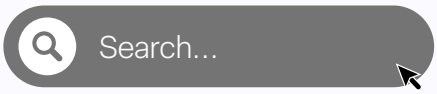
Confirmez l'article original.

Prenez le temps de vérifier l'exactitude du contenu avant de vous faire une idée ou de partager l'information.

Vérifiez également que les auteurs et les sources sont crédibles.

Utilisez les moteurs de recherche en ligne pour vérifier les informations.

Inscrivez des mots clés comme « canular », « fraude » ou « faux » dans votre recherche.



Comparez des informations provenant de sources multiples.

- ☐ Les informations sont-elles à jour ?
- ☐ Les informations sont-elles pertinentes par rapport aux événements actuels ?

Protégez-vous des cybermenaces.

- ☐ Installez un logiciel antivirus et un logiciel anti-programme malveillant réputés.
- ☐ Définissez des mots de passe forts et utilisez l'authentification multifactorielle.

Examinez les éléments de conception.

- ☐ La conception ne semble-t-elle pas bien réalisée ?
- ☐ Recherchez des logos non professionnels, des couleurs inhabituelles ou un espacement irrégulier.

✓ Canada

⊘ Canada

Validez les noms de domaine.

- ☐ L'adresse du lien correspond-elle au nom officiel de l'organisation ?
- ☐ Y a-t-il des fautes de frappe dans l'adresse du lien?

✓ **www.canada.ca**

⊘ **www.canada.net**

⊘ **www.canadaa.ca**

Tout le monde est susceptible de croire à la désinformation. Réfléchissez de manière critique aux informations que vous consommez et prenez des mesures pour vous assurer que les informations que vous communiquez sont exactes et fiables.

Même si la désinformation peut être difficile à repérer, portez attention à certains signes courants

Recherchez des contenus qui :

- **Provoquent une réaction émotionnelle, en particulier des affirmations négatives ou effrayantes**
- **Utilisent de petits éléments d'information valables qui sont exagérés ou déformés**
- **Manipulent des photos ou des images en les modifiant ou en les plaçant hors contexte**
- **Font une déclaration audacieuse ou extrême sur un sujet controversé**
- **Contient des « pièges à clics » :** des titres, des images et des vidéos sensationnels et délibérément trompeurs destinés à inciter les spectateurs à cliquer sur des liens spécifiques
- **Ont été largement communiqués sur des plateformes ayant l'habitude de diffuser de la désinformation**
- **Fait des affirmations qui semblent tout simplement trop belles pour être vraies**

Arrêtez la propagation de la désinformation

Soyez vigilant.

Dotez-vous des outils nécessaires afin de savoir comment déceler la désinformation.

Comprenez l'enjeu.

Comprenez le fonctionnement de l'Internet et des plateformes de médias sociaux et les efforts possibles pour manipuler les informations que vous consommez. Soyez aux aguets lorsque vous recevez de l'information. Soyez attentif aux signes courants, notamment les contenus qui : font une affirmation extraordinaire; semblent trop beaux pour être vrais; et ont été largement communiqués sur des plateformes ayant l'habitude de diffuser de la désinformation.

Faites la promotion d'une culture où on développe le réflexe de se baser sur des faits.

Démontrez que vous accordez de l'importance aux informations fondées sur les faits et encouragez les autres à faire de même.

Vérifiez vos sources.

Commencez par vérifier vos sources et voyez si des sources fiables rapportent les mêmes informations.
Vous trouverez des conseils et des ressources pour vous aider à vérifier les faits sur Canada.ca.

Signalez.

Toutes les plateformes de médias sociaux offrent aux utilisateurs un moyen de signaler la désinformation.

Pour en savoir plus sur la manière de vérifier les faits, de repéreret de contrer la désinformation, visitez le site Canada.ca/desinformation.

INGÉRENCE ÉTRANGÈRE

L'ingérence étrangère peut miner la confiance et menacer l'intégrité de nos institutions démocratiques, de notre système politique, de nos droits et libertés fondamentaux et, en fin de compte, de notre souveraineté.

Les acteurs étatiques ou non étatiques étrangers utilisent diverses techniques pour cibler tous les aspects de la société, comme les communautés diversifiées, les processus électoraux, les campus d'enseignement supérieur et les médias traditionnels et sociaux. Les techniques ou activités courantes utilisées par les acteurs étatiques étrangers peuvent comprendre la subtilisation de renseignements, la culture d'une relation, la coercition, le financement illicite, les cyberincidents, l'intimidation et la désinformation.

Contrairement à la coopération et à la diplomatie internationale légitime qui sont transparentes et faites de bonne foi, l'ingérence étrangère est secrète et malveillante. Voici d'autres signaux inquiétants à surveiller :

- un manque de transparence en ce qui concerne les communications, les relations, les comportements et les interactions;
- des suggestions ou des insinuations selon lesquelles l'interaction se traduira par un échange de faveurs ou d'avantages (contrepartie);
- des offres de cadeaux, de voyages ou d'autres avantages exceptionnellement généreux;
- des pressions visant à influencer d'autres personnes afin qu'elles soutiennent des points de vue, des opinions ou des positions particulières.

Protégez-vous et protégez votre ministère de l'ingérence étrangère

Soyez vigilant. Chacun a un rôle à jouer dans la lutte contre l'ingérence étrangère.

Soyez en sécurité sur Internet. Renseignez-vous sur la cybersécurité. Visitez le site pensezcybersecurite.gc.ca pour connaître les mesures à prendre pour vous protéger en ligne.

Vérifiez vos sources. Vérifiez la crédibilité de vos sources d'information pour vous assurer que vous recevez des informations exactes.

Signalez. Les activités suspectes et tout incident d'intimidation, de harcèlement, de coercition ou de menace doivent être signalés aux autorités locales chargées de l'application de la loi ou au Service canadien du renseignement de sécurité (SCRS).

Pour en savoir plus sur les moyens de se protéger contre l'ingérence étrangère, consultez Ingérence étrangère et vous et Protégez-vous contre l'ingérence étrangère.

Comment signaler l'ingérence étrangère au Canada

Toute personne au Canada qui craint d'être la cible d'acteurs étatiques ou non étatiques à des fins d'ingérence étrangère doit communiquer avec la police locale ou avec le **Réseau info-sécurité nationale de la Gendarmerie royale du Canada (GRC)** en composant le 1-800-420-5805 ou en écrivant à l'adresse suivante : RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca.

Signalez l'espionnage ou l'ingérence étrangère au **Service canadien du renseignement de sécurité (SCRS)** par téléphone, au 613-993-9620 ou au 1-800-267-7685, ou en ligne.

ISBN : 978-0-660-68167-2
CP22-207/1-2023F-PDF