Protéger la démocratie

Résister à **LA DÉSINFORMATION** et **L'INGÉRENCE ÉTRANGÈRE** trousse d'outils pour **LES FONCTIONNAIRES**

Désinformation

Fausses informations qui visent délibérément à induire en erreur.

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.

En tant que fonctionnaire, et selon l'objet de votre travail, vous pouvez être la cible d'activités de désinformation et d'ingérence étrangère. Les personnes qui participent à la prise de décisions sur les politiques publiques ou qui exercent une influence sur celles-ci sont des cibles tentantes.

Vous pouvez avoir accès à de l'information privilégiée, et il vous incombe de veiller à ce que ces renseignements soient conservés en toute sécurité.

Vous pouvez lutter contre la désinformation et protéger l'intégrité des institutions démocratiques du Canada en étant conscient de ces menaces et en prenant des mesures pour y répondre.

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

DÉSINFORMATION

Conseils sur la manière de distinguer les faits des fausses informations

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.

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

Soyez transparent. Reconnaissez que vous n'avez peut-être pas toute l'information ou que vous attendez toujours une confirmation.

Communiquez et faites la promotion des informations, des preuves et des contextes exacts. Faites en sorte que les informations exactes soient faciles à trouver et à comprendre.

Renforcez la résilience face à la désinformation comme suit :

- □ Comprenez l'environnement public.
- □ Collaborez avec d'autres personnes au sein de votre organisation afin de garantir la disponibilité d'informations exactes et cohérentes.

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.

La désinformation existe. Vous pourriez être une cible, alors restez vigilant. Dotez-vous des outils vous permettant de déceler et de combattre la désinformation et l'ingérence étrangère.

Soyez prêt.

Les organisations peuvent renforcer leur résilience grâce à la planification et en tenant compte des domaines prioritaires qui sont plus vulnérables à la désinformation. Reconnaissez ou anticipez d'éventuels récits trompeurs susceptibles de nuire à votre travail. Sachez où votre organisation peut être vulnérable.

- ☐ Commencez par déterminer les priorités de votre organisation qui pourraient être vulnérables à la désinformation.
- ☐ Comprenez l'environnement public. Consultez plusieurs sources d'information pour savoir ce qui se dit sur votre organisation, ainsi qu'où, comment et quand. Cela peut vous permettre de vous faire une idée précise de la nature et de la portée d'une question ou d'un sujet. Réalisez une analyse de l'environnement public pour vous aider à recueillir des informations et à rechercher des données auprès de nombreuses sources.
- ☐ Travaillez avec votre organisation pour élaborer des messages qui peuvent aider à lutter contre la désinformation avant qu'elle ne se produise.

Communiquez des faits fiables.

- ☐ Fournissez des informations exactes pour contrer la désinformation. Proposez des faits fiables de manière claire et efficace.
- ☐ Remplissez l'espace d'information avec des informations exactes et utiles, grâce à des communications fréquentes à l'aide de différentes méthodes, qui peuvent comprendre des conférences de presse et des séances d'information technique pour les médias, des fiches d'information pour fournir des informations supplémentaires et contextuelles, des mises à jour des sites Web du gouvernement, et des publications sur les comptes officiels des médias sociaux.
- ☐ Veillez à ce que votre message soit clair et concis. Utilisez un langage simple.

Rectifiez les faits.

Démystifier la désinformation signifie exposer directement les fausses informations, dans le but de clarifier les faits.

- ☐ Vérifiez les allégations à l'aide de sources crédibles et fournissez des contre-preuves précises pour contredire les fausses affirmations.
- ☐ Étayez les rectifications que vous apportez par des preuves et des sources crédibles. Fournissez des liens, des références ou des citations de sources réputées qui étayent vos affirmations.

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. Quels que soient le ministère, la classification ou le niveau, les fonctionnaires et les autres personnes qui participent au processus de prise de décision en matière de politique publique ou qui l'influencent peuvent être la cible d'acteurs étrangers.

Les acteurs étatiques étrangers utilisent diverses techniques pour cibler tous les aspects de la société civile, 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 internationales légitimes 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 proactif. Protégez-vous, protégez votre organisation, votre réputation et votre travail en étant conscient de la menace et en faisant preuve de diligence raisonnable.

Soyez prêt. Élaborez des politiques, des procédures et des processus pour traiter les cas d'ingérence étrangère. Rendez-les publiques afin que les acteurs potentiels de la menace sachent que vous ne tolérerez pas les activités d'ingérence étrangère. Vous pouvez consulter les responsables de la sécurité de votre ministère et les politiques en vigueur au sein de votre organisation.

Éduquez. Fournissez des documents de sensibilisation, des formations et des conseils sur les politiques et procédures connexes à l'ensemble des employés et des entrepreneurs.

Signalez. Les activités suspectes et tout incident d'intimidation, de harcèlement, de coercition ou de menace doivent être signalés au dirigeant principal de la sécurité de votre ministère, aux autorités locales chargées de l'application des lois 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)** en composant le 613-993-9620 ou le 1-800-267-7685, ou en ligne.

ISBN : 978-0-660-68171-9
CP22-207/3-2023F-PDF