Repérer les cas de mésinformation, désinformation et malinformation

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

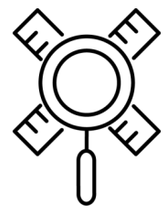
Mai 2024 | ITSAP.00.300

Chaque année, l'économie mondiale est privée de milliards de dollars à cause de cas de mésinformation, désinformation et malinformation (MDM). Aussi appelées « infox » ou « fausses nouvelles », les activités de MDM fragilisent la confiance du public dans les institutions et peuvent même, en période électorale, mettre la démocratie en péril. Elles sont maintenant une grave source de préoccupation pour les consommatrices, les consommateurs et les organisations de toute taille. De nouvelles technologies, comme l'apprentissage automatique, le traitement automatique des langues et les réseaux d'amplification, sont utilisées pour discréditer de l'information factuelle. L'intelligence artificielle (IA) et l'IA générative peuvent aussi servir à mener des campagnes de désinformation et à diffuser de l'information fausse et trompeuse, notamment par l'hypertrucage. Le présent document explique comment repérer les cas de MDM et énumère les mesures de sécurité que les consommatrices, les consommateurs et les organisations peuvent prendre pour contrer les risques.

Types d'information

- L'information **valide** est factuellement exacte, repose sur des données qui peuvent être confirmées et ne prête aucunement à confusion.
- L'information **inexacte** est incomplète ou manipulée de sorte à transmettre une fausseté.
- L'information **fausse** est incorrecte et peut être réfutée avec des données.
- L'information **non vérifiable** est impossible à confirmer ou à réfuter en se fondant sur des données existantes.

Définir la mésinformation, la désinformation et la malinformation



Il y a trois types d'activités de MDM qui peuvent entraîner des préjudices mineurs ou graves.

La **mésinformation** désigne le fait de diffuser de la fausse information sans avoir de mauvaises intentions.

La **désinformation** réfère au fait de diffuser de la fausse information dans le but de manipuler ou de tromper des personnes, des organisations et des États ou bien de leur faire du tort.

La **malinformation** consiste à diffuser de l'information qui repose sur un fait, mais qui est souvent exagérée de façon à tromper ou même à causer des préjudices.

Éléments à surveiller

Pour déceler la MDM, évaluez rigoureusement le contexte de l'information et prenez le temps d'en examiner la source et le message. Lorsque vous lisez du contenu, peu importe sa forme, posez-vous les questions suivantes :

- Le contenu provoque-t-il une réaction émotionnelle?
- Contient-il des propos osés sur une question controversée?
- Contient-il des affirmations étonnantes?
- Contient-il des pièges à clics?
- Repose-t-il sur de petits fragments d'information valide qui sont exagérés ou déformés?
- Est-il devenu viral sur des plateformes sur lesquelles la surveillance est déficiente, voire inexistante?

Ces quelques questions peuvent vous aider à déterminer si vous avez affaire à un cas de MDM. Même si vous répondez par l'affirmative à l'une des questions, ne rejetez pas l'information pour autant. Vous devez simplement approfondir votre recherche sur le contenu avant de vous y fier.

Cibles et victimes

Pour protéger votre organisation, il est crucial de bien comprendre les cibles de la MDM et la manière dont les auteures et auteurs de menace utilisent la MDM. Consultez le document Tactics of disinformation publié par nos partenaires à la CISA (en anglais seulement).

Les auteures et auteurs de menace étrangers utilisent la MDM pour ébranler la confiance dans les espaces virtuels et pour influencer le discours international. Les principales **cibles** des campagnes de désinformation sont les membres des communautés linguistiques minoritaires et les membres des diasporas. L'idée est d'utiliser les différences sociales et culturelles pour déstabiliser les systèmes politiques.

Les femmes sont **davantage ciblées** par la MDM. Les auteures et auteurs de menace utilisent souvent les hypertrucages sexualisés pour humilier et dégrader les femmes dans les sphères publiques et politiques. Consultez la publication Désinformation genrée : Tactiques, thèmes et tendances des acteurs malveillants étrangers pour en apprendre davantage sur ce sujet.

Hypertrucages

L'hypertrucage est une tactique de plus en plus utilisée par les auteures et auteurs de cybermenace. Il réfère à un contenu synthétique qui a été manipulé par des moyens numériques dans le but de tromper les gens. Les hypertrucages peuvent comprendre des images, du contenu audio ou des vidéos générés artificiellement et être utilisés à la place des images, du contenu audio ou des vidéos originaux. La technologie évolue rapidement et les hypertrucages deviennent plus faciles à créer et plus difficiles à détecter. Même si l'IA peut faciliter la création de MDM, elle peut aussi servir d'outil essentiel pour détecter la fausse information. L'IA peut examiner les métadonnées d'un fichier, d'une photo ou d'une vidéo pour ensuite déterminer sa provenance.

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

© Sa Majesté le Roi du chef du Canada, représenté par le ministre de la Défense nationale, [2024]

Cat. No. D97-1/00-300-2024F-PDF
ISBN 978-0-660-71532-2

Canada

Repérer les cas de mésinformation, désinformation et malinformation

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mai 2024 | ITSAP.00.300

Passer à l'action en tant que consommatrice ou consommateur

- Consultez un site de vérification des faits pour déterminer si l'information en question a déjà été réfutée.
- Lancez une recherche d'image inversée pour confirmer que les images n'ont pas été copiées d'un site Web ou d'une organisation légitime.
- Ne supposez pas que l'information que vous recevez est correcte, même si elle provient d'une source valide (comme un ami ou un proche).
- Soyez à l'affût des éléments graphiques inadaptés à la situation, comme des logos, des couleurs, des espacements et des GIF animés qui n'ont pas l'air professionnels.
- Vérifiez les noms de domaine pour vous assurer qu'ils correspondent à ceux de l'organisation. Le nom de domaine peut être légèrement différent ou avoir un domaine de premier niveau (TLD) différent, comme .net ou .org.
- Confirmez que l'organisation a publié des coordonnées, une adresse physique et une page « À propos de nous ».
- Effectuez une recherche dans WHOIS pour déterminer à qui appartient le domaine et vérifier si l'organisation propriétaire est digne de confiance. WHOIS est une base de données qui contient des détails sur les noms de domaine, soit leur propriétaire, leur date d'enregistrement et leur date d'expiration.
- Assurez-vous que l'information est à jour.

Passer à l'action en tant qu'organisation

- Faites de la surveillance dans les médias sociaux et en ligne et souscrivez à des services d'alerte qui repèrent et suivent les fausses nouvelles concernant votre organisation. Souvent, ces services vous laissent surveiller non seulement vos profils de médias sociaux, mais aussi les publications publiques, les forums en ligne, les sites Web, les évaluations, les mentions, etc.
- Utilisez l'optimisation pour les moteurs de recherche et affichez du contenu transparent et de grande qualité partout sur le Web. Vous pourrez ainsi améliorer le placement de votre site Web et de vos médias sociaux dans les moteurs de recherche (comme Google). Grâce à cette technique, votre site pourrait s'afficher avant, plutôt qu'après, un site Web qui vise votre organisation avec des activités de MDM.
- Utilisez l'optimisation pour les moteurs de réponse qui vise surtout les assistants vocaux personnels. L'objectif est d'optimiser les réponses données par ces dispositifs pour qu'ils relatent des faits sur votre organisation plutôt que de la fausse information.
- Recourez à des réseaux d'amplification pour augmenter la portée et la visibilité de votre contenu et éviter que la fausse information prenne le dessus sur la réalité. Les réseaux d'amplification s'apparentent à des haut-parleurs pour la vérité, et ils peuvent se composer de partenaires organisationnels, d'ambassadrices et ambassadeurs de marque et de clientes et clients actuels.
- Favorisez la coopération avec vos clientes, clients, utilisatrices et utilisateurs pour vous assurer de l'établissement et du maintien de la confiance. Par exemple, les moteurs de recherche se servent des évaluations faites par des clientes, clients, utilisatrices et utilisateurs pour mesurer la fiabilité d'une marque.
- Mettez sur pied une équipe d'intervention qui contrera indirectement toute campagne de MDM et veillera à ce qu'une riposte soit amorcée le plus rapidement possible.
- Évitez de répondre directement à de la MDM.
  - Votre réponse doit être de nature passive et ne doit pas être affichée dans la même conversation, la même publication ou le même fil que le cas de MDM.
  - Visez plutôt à répondre sur votre site Web.
  - Assurez-vous que votre réponse à de la MDM contient des réponses détaillées, transparentes et factuelles.

Pour en savoir plus

Pour obtenir des conseils et des ressources en lien avec la MDM, vous pouvez consulter les publications suivantes :

- Réalité ou invention? Conseils pour vous aider à repérer les fausses nouvelles
- ITSAP.00.040 : Intelligence artificielle
- ITSAP.00.41 : L'intelligence artificielle générative
- ITSAP.00.101 : Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage
- Évaluation des cybermenaces nationales 2023-2024
- La désinformation en ligne (GC)
- Les cybermenaces contre les élections (GC)
- Renforcer le système électoral canadien (GC)
- Intégrité et sécurité des élections, y compris l'ingérence étrangère (Élections Canada)

Centre de la sécurité des télécommunications Canada | Communications Security Establishment Canada

© Sa Majesté le Roi du chef du Canada, représenté par le ministre de la Défense nationale, [2024]

Canada