REPÉRER LES CAS DE MÉSINFORMATION, DÉSINFORMATION ET MALINFORMATION

Novembre 2021

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 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, comme l'hypertrucage, peut aussi servir à mener des campagnes de désinformation et à diffuser de l'information fausse et trompeuse. Par hypertrucage, on entend des images, du contenu audio ou des vidéos générés artificiellement et utilisés à la place des images, du contenu audio ou des vidéos originaux. Le présent document explique comment repérer les cas de MDM et énumère les mesures de sécurité que les consommateurs et les organisations peuvent prendre pour en atténuer les risques.

COMMENT REPÉRER LES CAS DE MDM?

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

- Est-ce que le contenu provoque une réaction émotionnelle?
- Est-ce qu'il contient des propos osés sur une question controversée?
- Est-ce qu'il contient des affirmations étonnantes?
- Est-ce qu'il contient des pièges à clics?
- Est-ce qu'il contient de l'information pertinente en fonction du contexte?
- Est-ce qu'il repose sur de petits fragments d'information valide qui sont exagérés ou déformés?
- Est-ce qu'il est devenu viral sur des plateformes sur lesquelles la surveillance est déficiente, voire inexistante?

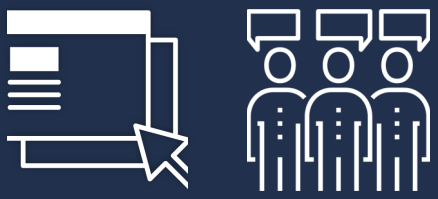
Il s'agit là de quelques questions qui peuvent vous aider à déterminer si vous avez affaire à un cas de MDM. Même si vous répondez par l'affirmative à une des questions, ne rejetez pas l'information pour autant. Vous devez simplement approfondir votre recherche sur le contenu avant de vous y fier.

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.

Par **désinformation**, on entend le 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.

Pour ce qui est de la **malinformation**, il s'agit du fait de diffuser de l'information qui repose sur un fait, mais qui est souvent exagérée de façon à tromper ou même à causer des préjudices.



Lorsque de l'information est **valide**, elle est factuellement exacte, repose sur des données qui peuvent être confirmées et ne prête aucunement à confusion.

L'information est **inexacte** lorsqu'elle est incomplète ou manipulée de sorte à transmettre une fausseté.

L'information **fausse** est incorrecte et peut être réfutée avec des données.

L'information est non **vérifiable** lorsqu'il est impossible de la confirmer ou de l'infirmer en se fondant sur les données existantes.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-300-2022F-PDF
ISBN 978-0-660-42183-4

QUELLES MESURES LES CONSOMMATEURS PEUVENT-ILS PRENDRE POUR CONTRER LES ACTIVITÉS DE MDM?

En tant que consommateur d'information, vous pouvez vérifier le contenu et vous protéger contre les cas de MDM en appliquant les mesures suivantes :

- Cherchez pour des éléments graphiques inadaptés à la situation, comme des logos, des couleurs, des espacements et des gifs animés qui n'ont pas l'air professionnels.
- Vérifiez si le nom de domaine correspond à celui de l'organisation en question. 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.
- 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.
- Consultez un site de vérification des faits pour déterminer si l'information en question a déjà été infirmée.
- 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).
- Vérifiez si l'information est toujours pertinente.

POUR EN SAVOIR PLUS

Pour obtenir des conseils et des ressources concernant les activités de MDM, vous pouvez consulter les publications suivantes sur notre site Web :

- *Réalité ou invention? Conseils pour vous aider à repérer les fausses nouvelles*
- *Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)*
- *La COVID-19 et les sites Web malveillants (ITSAP.00.103)*
- *Considérations de sécurité relatives au développement et à la gestion de votre site Web (ITSAP.60.005)*

QUELLES MESURES LES ORGANISATIONS PEUVENT-ELLES PRENDRE POUR CONTRER LES ACTIVITÉS DE MDM?

Les organisations peuvent se protéger contre la menace que représentent les activités de MDM en appliquant les stratégies et les mesures suivantes :

- 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 comme Google Home, Amazon Alexa et Siri. 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'ambassadeurs de marque et de clients actuels.
- Sollicitez l'engagement de vos clients et de vos utilisateurs pour confirmer la présence et le maintien du lien de confiance. Par exemple, les moteurs de recherche se servent des évaluations faites par des clients et des 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.
- Ne réagissez pas directement à un cas de 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. Vous pourriez plutôt réagir sur votre site Web, par exemple. Assurez-vous que votre réponse contient des réponses détaillées, transparentes et factuelles. Cela peut varier en fonction de l'organisation.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.