How to identify misinformation, disinformation and malinformation

CANADIAN CENTRE FOR CYBER SECURITY

May 2024 | ITSAP.00.300

The effects of misinformation, disinformation, and malinformation (MDM) cost the global economy billions of dollars each year. Often known colloquially as “fake news”, MDM is damaging to public trust in institutions and, during elections, may even pose a threat to democracy itself. MDM has become a serious concern for consumers and organizations of all sizes. New technologies such as machine learning, natural language processing, and amplification networks are being used to discredit factual information. Disinformation campaigns may use artificial intelligence (AI) and generative AI to spread false and misleading information, such as deepfakes. This document offers consumers and organizations information on identifying MDM and implementing the appropriate security measures to counter it.

Types of information

Valid information means that it is factually correct, is based on data that can be confirmed, and isn’t misleading in any way.

Inaccurate information is either incomplete or manipulated in a way that portrays a false narrative.

False information is incorrect and there is data that disproves it.

Unsustainable information can neither be confirmed nor disproved based on the available data.

What to look for

Evaluate the information landscape critically and take the time to review the sources and messaging.

When viewing content, in any form, ask yourself the following questions:

- Does it provoke an emotional response?
- Does it make a bold statement on a controversial issue?
- Is it an extraordinary claim?
- Does it contain clickbait?
- Does it have topical information that is within context?
- Does it use small pieces of valid information that are exaggerated or distorted?
- Has it spread virally on unvetted or loosely vetted platforms?

These are a few guiding questions that can help you identify MDM. Even if one of these questions applies to a source, it does not automatically discredit the information. It is an indication to conduct more research on the item before trusting it.

Defining misinformation, disinformation and malinformation

MDM can be identified as three main forms of informational activity that can cause minor or major harm.

Misinformation refers to false information that is not intended to cause harm.

Disinformation refers to false information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction.

Malinformation refers to information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm.

Targets and victims

Understanding who might be targeted and how threat actors use MDM is crucial for protecting your organization. Check out [Tactics of disinformation] from our partners at CISA.

Foreign actors use MDM to reduce trust in online spaces and influence international narratives. Primary **target recipients** for disinformation campaigns are members of linguistic minorities and diasporic communities. The idea is to use social and cultural differences to destabilize political systems.

Women, are disproportionately **targeted subjects** of MDM. Hyper-sexualized deepfakes are frequently used to shame and undermine women in public and political spheres. Check out Gendered disinformation: Tactics, themes, and trends by foreign malign actors to learn more about this issue.

Deepfakes

Deepfakes are becoming an increasingly common tactic used by cyber threat actors. They refer to Synthetic content that has been digitally manipulated and is intended to deceive. This includes artificially generated images, audio and videos used in place of the original content. Technology is evolving rapidly and deepfakes are getting easier to make and harder to detect. While AI facilitates the creation of MDM, it is also an integral tool to help detect false information. AI can examine the metadata of a file, photo or video and can provide information on its source.

Cat. No. D97-1/00-300-2024E-PDF
ISBN 978-0-660-71531-5

How to identify misinformation, disinformation and malinformation

CANADIAN CENTRE FOR CYBER SECURITY

May 2024 | ITSAP.00.300

Taking action as a consumer

- Use a fact–checking site to ensure the information you are reading has not already been proven false.
- Conduct a reverse image search to ensure images are not copied from a legitimate website or organization
- Don't automatically assume information you receive is correct, even if it comes from a valid source (such as a friend or family member)
- Look for out of place design elements such as unprofessional logos, colours, spacing, and animated gifs
- Verify domain names to ensure they match the organization. The domain name may have typos or use a different Top Level Domain (TLD) such as .net or .org
- Check that the organization has contact information listed, a physical address and an "About Us" page
- Perform a WHOIS lookup on the domain to see who owns it and verify that it belongs to a trustworthy organization WHOIS is a database of domain names and has details about the owner of the domain, when the domain was registered, and when it expires
- Ensure the information is up to date

Taking action as an organization

- Set up social media, web monitoring and alerting services for identifying and tracking fake news related to your brand and organizations. These services often let you monitor not only your own social media profiles, but also public posts, web forums, websites, reviews, mentions, etc.
- Use search engine optimization (SEO) along with transparent, high quality content on any web presence. SEO is used to optimize your site and social media listings on search engines such as Google and can ensure that your website is being displayed higher than a website with MDM that is targeting your organization
- Use answer engine optimization (AEO) which focuses on voice assistants to optimize answers from these devices so that they point to facts about your organization and not false information
- Use amplification networks to increase the reach and visibility of your content and prevent false information from overpowering the truth. Amplification networks act as loudspeakers for the truth and can include organizational partners, brand ambassadors, and existing customers
- Encourage engagement with your customers and users to ensure trust is established and maintained. For example, search engines use reviews by customers and users to gauge the trustworthiness of a brand
- Create a response team to indirectly counteract any MDM campaigns and ensure a response occurs as soon as possible.
- Avoid directly engaging with MDM
  - Responses should be passive in nature and not within the conversation, post or thread that they are posted on
  - Opt to post your response on your website instead
  - Ensure that a response to MDM includes detailed, transparent and factual answers.

Learn more

To find additional guidance and resources regarding MDM, refer to the following resources:

- Fact or fiction: Quick tips to help identify "fake news"
- ITSAP.00.040: Artificial intelligence
- ITSAP:00.41: Generative artificial intelligence (AI)
- ITSAP.00.101: Don't take the bait: Recognize and avoid phishing attacks
- National Cyber Threat Assessment 2023-2024
- Online disinformation (GC)
- Cyber threats and elections (GC)
- Protecting democracy (GC)
- Election integrity and security including foreign interference (Elections Canada)