Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

February 2022

HOW TO IDENTIFY MISINFORMATION, DISINFORMATION, AND MALINFORMATION

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 are 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) to spread false and misleading information, such as deepfakes. Deepfakes refer to artificially generated images, audio, and videos used in place of the original image, audio, or video. This document offers consumers and organizations information on identifying MDM and implementing the appropriate security measures for mitigation strategies.

HOW TO IDENTIFY MDM

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?

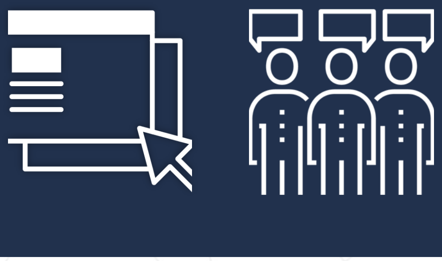
These are a few guiding questions that can help you identify MDM. Even if one of these questions applies to a source, it does not automatically discredit the information. It is an indication to conduct more research on the item before trusting it.

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.



Information that is **valid** means that it is factually correct, is based on data that can be confirmed, and is not 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.

Cat. No. D97-1/00-300-2022E-PDF
ISBN 978-0-660-42182-7

HOW CAN CONSUMERS TAKE ACTION AGAINST MDM?

As a consumer of information, you can take these actions to investigate content further and protect yourself from MDM:

- 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.
- Conduct a reverse image search to ensure images are not copied from a legitimate website or organization.
- Use a fact–checking site to ensure the information you are reading has not already been proven false.
- Do not automatically assume information you receive is correct, even if it comes from a valid source (such as a friend or family member).
- Ensure the information is not out of date.

LEARN MORE

To find additional guidance and resources regarding MDM, you may refer to the following publications on our website (https://cyber.gc.ca/en/publications):

- *Fact or Fiction: Quick Tips to Help Identify "Fake News"*
- *Developing your incident response plan (ITSAP.40.003)*
- *COVID-19 and Malicious Websites (ITSAP.00.103)*
- *Security considerations when developing and managing your website (ITSAP.60.005)*

HOW CAN ORGANIZATIONS TAKE ACTION AGAINST MDM?

Organizations can protect themselves from the threat of MDM by applying the following strategies and controls:

- Set up social media and web monitoring, as well as 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 make the difference of being displayed above or below a website with MDM that is targeting your organization.
- Use answer engine optimization (AEO) which focuses on voice assistants such as Google Home, Amazon Alexa, or Siri 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.
- Do not directly engage with MDM. Responses should be passive in nature and not within the conversation, post, or thread that they are posted on. Instead, you could post the response on your website. Ensure that a response to MDM includes detailed, transparent, factual answers. This may vary depending on the organization.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**