

Protecting Democracy

Toolkit to resist **DISINFORMATION** and **FOREIGN INTERFERENCE** for community leaders

Disinformation

False information that is deliberately intended to mislead.

Foreign Interference

Deliberate and covert activities by foreign groups, state actors, or individuals to advance their interests, often to the detriment of Canada's national interests.

Our best defence against disinformation and foreign interference is to build resilience through awareness and understanding.

In Canada and around the world, democracy and democratic institutions (e.g. Parliament, provincial legislatures, the electoral process) have long faced threats from people or groups whose goal is to weaken them and weaken citizens' trust in government.

This includes disinformation - the deliberate spread of inaccurate information - and foreign interference, which have a negative effect on the well-being of people living in Canada and on Canada's unity.

You can protect yourself and others by becoming aware of the threats of disinformation and foreign interference, learning how to identify false information, and understanding how information is shared and consumed online.

For more information and resources, visit [Protecting Canada's democratic institutions](#) and [Foreign Interference](#).



DINSINFORMATION

Tips on how to spot disinformation

Confirm the original story.

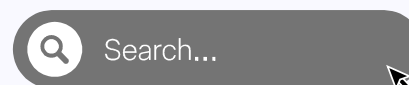
Pause to consider the accuracy of content before drawing conclusions or sharing.

Also check to make sure that the authors and sources are credible.



Use online search engines to verify information.

Include key words such as “hoax,” “scam,” or “fake” in your search.



Compare information from multiple sources.

- Is the information current?
- Is the information relevant to present events?



Protect yourself from cyber threats.

- Install reputable antivirus and malware software.
- Set strong passwords and use multi-factor authentication.



Look at the design elements.

- Does the design look out of place?
- Look for unprofessional logos, unusual colours, or odd spacing.



Validate domain names.

- Does the link address match the official name of the organization?
- Are there any typos in the link address?

- ✓ www.canada.ca
- ✗ www.canada.net
- ✗ www.canadaa.ca



Everyone is susceptible to believing disinformation. Think critically about the information you consume and take steps to make sure the information that you share is accurate and reliable.

Disinformation can be hard to spot, but there are some common signs to watch for

Look for content that:

Provokes an emotional response, particularly with negative or frightening claims

Uses small pieces of valid information that are exaggerated or distorted

Manipulates photos or images by altering them or placing them out of context

Makes a bold or extreme statement on a controversial issue

Contains “clickbait”: sensational and purposefully misleading headlines, images, and videos meant to entice viewers to click on specific links

Has been shared widely on platforms with a track record of spreading disinformation

Makes claims that simply seem too good to be true

Stop the spread of disinformation

Be aware.

Equip yourself with the necessary tools in order to identify disinformation.

Understand it.

Understand how the internet and social media platforms work and possible efforts to manipulate the information you consume. Be vigilant when receiving information. Watch for the common signs including content that: makes an extraordinary claim; seems too good to be true; and has been shared widely on platforms with a track record of spreading disinformation.

Promote a culture of accuracy.

Demonstrate that you value the accuracy of information and encourage others to do the same.

Verify your sources.

Start by checking your sources and see if reliable sources are reporting the same information. You can [find tips and resources to help you fact-check your information](#) on Canada.ca.

Report it.

All social media platforms give users a way to report disinformation.

Visit [Online disinformation](#) for more information on how to identify, fact-check and counter disinformation.



FOREIGN INTERFERENCE

Foreign interference can erode trust and threaten the integrity of our democratic institutions, political system, fundamental rights and freedoms, and ultimately, our sovereignty.

Foreign state or non-state actors use a variety of techniques to target all aspects of society, such as diverse communities, electoral processes, post-secondary campuses, and traditional and social media. Common techniques or activities used by foreign state actors can include: elicitation, cultivation, coercion, illicit financing, cyber-incidents, intimidation and disinformation.

Unlike legitimate international cooperation and diplomacy which is transparent and done in good faith, foreign interference is covert and malign. Some other concerning signals to watch for include:

- a lack of transparency around communications, relationships, behaviour and interactions
- suggestions or implications that interaction will result in an exchange of favours or advantages (quid pro quo)
- offers of unusually generous gifts, travel or other benefits
- pressure to influence others to support particular views, opinions or positions.

Protect yourself from foreign interference

Be alert. Everyone has a role to play in the fight against foreign interference.

Be cyber safe. Educate yourself about cyber security. Visit [Get Cyber Safe](#) for steps you can take to protect yourself online.

Verify your sources. Check the credibility of your information sources to ensure that you are receiving accurate information.

Report it. Suspicious activities and any incidents of intimidation, harassment, coercion, or threats should be reported to your local law enforcement authorities or the Canadian Security Intelligence Service (CSIS).

For more information on ways to protect yourself from foreign interference, consult [Foreign Interference and You](#) and [Protect yourself from foreign interference](#).

How to report foreign interference in Canada

Any individual in Canada who is concerned that they are being targeted by state or non-state actors for the purposes of foreign interference should contact local police or the **Royal Canadian Mounted Police's (RCMP) National Security Information Network** at 1-800-420-5805, or by email at RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca.

Report espionage or foreign interference to the **Canadian Security Intelligence Service (CSIS)** at 613-993-9620 or 1-800-267-7685, or [online](#).

© His Majesty the King in Right of Canada, 2023.
ISBN: 978-0-660-68166-5
CP22-207/1-2023E-PDF

Also available in French
and other languages.

