Protecting Democracy

Toolkit to resist DISINFORMATION and FOREIGN INTERFERENCE for ELECTED OFFICIALS and PUBLIC OFFICE HOLDERS

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.

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.

As an elected official or a public office holder, you may become a target of disinformation. Individuals with input into or influence over the public policy decision-making process are attractive targets.

You may have access to privileged information and it is your responsibility to ensure that the information is kept safe. It is important to provide your team with resources and training so they are aware of threats and have the tools combat them.

For more information and resources, visit canada.ca/protecting-democratic-institutions and publicsafety.gc.ca.

DINSINFORMATION

Tips on how to spot disinformation

Promote a culture of accuracy. Demonstrate that you value accurate information and encourage others to do the same.

Pause before sharing. Take a moment to consider the accuracy of content and sources before drawing conclusions or sharing.

Set up social media monitoring and alert services. This allows you to identify and track disinformation related to your name, office, or organization. Monitor not only your social media profiles, but also public posts, web forums, websites, reviews, mentions, and so on. Consult reputable disinformation-monitoring organizations such as the EUvsDisinfo, DisinfoWatch, and Global Affairs Canada's Rapid Response Mechanism. Conduct reverse image searches.

Create a response team. Ensure your staff is prepared to identify and respond to disinformation campaigns quickly and effectively.

Know your audience. Communicating in a way that shows that you understand your audience will increase the chances of your information being understood.

Be selective when directly engaging with disinformation on social media. Doing so can contribute to the spread of the disinformation. Instead, your response to disinformation should be posted in a separate thread or post and should be detailed, transparent, and accurate. You could also post the response on your website.

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 of 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.

Disinformation is out there. You could be a target so always be on the lookout. Equip yourself with the tools to know how to identify and combat disinformation.

Be prepared.

- ☐ Determine the key business lines and areas in your organization/office that may be vulnerable to the spread of disinformation.
- ☐ Understand the public environment. Consult multiple sources of information to know what is being said about your office/organization, as well as where, how, and when it is being said. This can give you a clearer picture of the nature and scope of an issue or subject. Conduct a public environment analysis (PEA) to help you gather information and research data from numerous sources.
- ☐ Develop messaging in advance to address potential disinformation narratives.

Communicate.

- ☐ Provide accurate information when countering disinformation. Make sure to offer correct and reliable facts
- ☐ Communicate in a timely manner.
- ☐ Consider the best means of communication. You may want to address false information by providing factual information that explicitly counters the disinformation using your social media platform, a press release or you may wish to engage with your media relations team to work with media outlets to clarify miscommunication.
- ☐ Ensure your messaging is clear and concise.

Correct it.

To debunk disinformation means to expose false information, directly, with the aim of clarifying the facts.

- ☐ Fact-check claims by using credible sources and provide accurate counterevidence to the false narrative.
- ☐ Back up your corrections with credible sources and evidence. Provide links, references, or citations to reputable sources that support your statements.

FOREIGN INTERFERENCE

Foreign interference involves foreign states, or persons acting on their behalf, whose goal it is to covertly influence decisions, policy, or events within Canada to advance their own interests. This can erode trust and threaten the integrity of our democratic institutions, political system, fundamental rights and freedoms, and ultimately, our sovereignty.

State actors may use deceptive means to develop trusted relationships with elected officials, their staff or candidates in order to covertly obtain privileged information, shape debate or influence decision making in a way that is advantageous to a foreign state. These relationships are often developed early in one's political career to gain a level of trust that is exploited later on. In other cases, state actors may use coercive tactics. This can happen over time, and it can be hard to spot. Awareness of this risk is critical given anyone, at any level of government, can be a potential target.

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

For more information, consult: Foreign Interference Threats to Canada's Democratic Process.

Protect yourself from foreign interference

Be alert. The resilience of Canada's democracy is a responsibility we all share. Know the warning signs of foreign interference.

Research. Do your due diligence before sharing information or entering into arrangements, know your partners and assess the risks of any partnership in advance.

Be proactive. Protect yourself, your organization, your reputation, and your work by being aware of the threat and performing due diligence.

Be cyber safe. Educate yourself about cyber security. Visit getcybersafe.gc.ca 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 as well as to 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.

ISBN: 978-0-660-68168-9
CP22-207/2-2023E-PDF