Protecting Democratic Institutions
Tool kit to resist disinformation and foreign interference
for Elected Officials and Public Office Holders

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

In Canada and around the world, our 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.

Disinformation	Foreign interference
False information that is deliberately intended to mislead, also referred to as fake news.	Deliberate and covert activities by foreign groups, state actors, or individuals to advance their interests, often to the detriment of Canada's national interests.

As an elected official or a public office holder, you may become a target of disinformation and foreign interference. 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.

Tips on how to separate facts from false information online:

- **Set up social media monitoring and alert services**. This allows you to identify and track fake news 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.
- **Create a response team.** This team will work to identify and debunk disinformation campaigns and should be poised to respond quickly.
- **Do not directly engage with disinformation on social media**. Doing so will contribute to the spread of the disinformation. Instead, your response to disinformation should be posted in a separate thread or post and should include be detailed, transparent, and accurate. You could also post the response on your website.
- **Know your audience.** Communicating in a way that shows that you understand your audience will increase the chances of your information being understood.
- **Don't be a passive target for foreign interference**. Protect yourself, your organization/office, your reputation, and your work by being aware of the threat and doing your due diligence.

Disinformation can be hard to spot, but there are some common signs to watch for. Look for content that:

- Provokes an emotional response -> "Nobody likes hockey anymore!"
- Makes a bold statement on a controversial issue -> "Government bans pineapple on pizza calling it an abomination!"
- Makes an extraordinary claim -> "Did you know? An adult foot grows half a shoe size in the summer?"
- Has been shared widely on platforms with a track record of spreading disinformation -> "Trooth Now: your source for all the latest newz!"
- Uses small pieces of valid information that are exaggerated or distorted -> "Vitamin A can help with night vision, take it every day and never buy another flashlight again!"
- Contains clickbait -> "You won't believe this video!"
- Seems too good to be true -> "Government of Canada buildings offering free ice cream cones to first 1,000, 000 visitors!"

Stop the spread of disinformation:

Be aware. Disinformation and foreign interference are 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 and foreign interference.

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 by consulting several sources of information to know what is being said, where, and when it is being said about you or your office/organization. This provides a clear 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. To learn more about PEA, visit www.canada.ca/en/privy-council/services/communications-community-office/communications-101-boot-camp-canadian-public-servants/strategic-thinking-communications.html.
- ☐ 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 respond to false information directly 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 can erode trust and threaten the integrity of our democratic institutions, political system, fundamental rights and freedoms, and ultimately, our sovereignty. Foreign interference threats affect all levels of government and target all facets of Canadian society, including civil society, communities, media, voters, political parties, candidates, elected officials and their staff, and elections themselves.

State actors may use deceptive means to develop a relationship with electoral candidates or their staff to covertly obtain information to be used later to their advantage through, for example, threats and blackmail. Alternatively, a state actor may decide to recruit the individual over time in the hopes of achieving greater gains if the individual is elected. After a long period of cultivation there are more opportunities to gain control over the official which can be used to pressure the individual into influencing debate and decision-making within government. The individual may also be able to hinder or delay initiatives that are contrary to the foreign state's interest.

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

Protect yourself from foreign interference:

Learn. Increasing our collective resilience against foreign interference is a shared responsibility.

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 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*.

How to report foreign interference in Canada

In the case of an **immediate threat** to your personal safety or the safety of a member of your family, **call 911**.

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, online at www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html.