Protecting Democracy

RESISTING DISINFORMATION DURING AN ELECTION

Our best defence against disinformation is to be aware and build resilience.

Voters may be targeted overtly or covertly by foreign actors who spread disinformation to influence their vote. Their goal is to manipulate people, spread fake news and create conflict to sow doubt in the election process.

Here are some ways you can protect yourself against the threat of disinformation.

What is disinformation?

Disinformation is false information that is deliberately intended to mislead the reader. Online disinformation can be hard to spot, so pay close attention to any content that:

- Provokes an emotional response in you, particularly with negative or frightening claims.
- Uses satire, like memes, that could be misinterpreted as factual.
- Makes a bold or extreme statement on a controversial issue.
- Contains “clickbait”, which is purposefully misleading headlines, images, and videos, meant to entice you to click on specific links.
- Makes claims that are simply too good to be true.

© His Majesty the King in Right of Canada, as represented
by the Minister of Democratic Institutions, 2025.
ISBN: 978-0-660-76070-4 | CP22-229/2025E-PDF

How is disinformation spread during elections?

Deepfakes are fake videos, images or audio recordings created using artificial intelligence (AI) to spread false information.

Deepfakes can depict real or non-existent people, like political figures or journalists, and can be very convincing. For example, a deepfake video might show a candidate saying something offensive or inappropriate, even though they never actually said it, all with the intent to influence voters’ opinions.

Misleading images, videos and audio can be used to create false narratives through visual and audio manipulation. For example, old photos or videos can be repurposed to represent current events or images could be edited to exaggerate the effects of real events. Images and videos could also be taken out of context to mislead viewers.

An audio recording, generated using AI voice-cloning technology, could be used to mimic a candidate’s voice but fabricating words entirely. By the time the truth emerges, the damage is already done — public trust in the candidate has been shaken and some people believe the false narrative.

Fake accounts and bots can be used to amplify disinformation or give the illusion of widespread support. Bots can be used to spread identical messages supporting or opposing a narrative or a policy. Fake accounts are often used to pose as real people to spread disinformation about social issues.

Disinformation campaigns using fake social media accounts and bots could be used to influence public opinions during elections. They target specific groups, by impersonating people, to exploit social divisions. These accounts could be used to spread false narratives, including conspiracy theories, with the goal of sowing distrust in democratic institutions.

Social content creators and influencers can be targeted by threat actors to spread false narratives and manipulated information onto their audiences. Their endorsements shape opinions, especially among audiences who rely on social media and online platforms for news.

Unlike product promotions, influencers aren’t legally required to disclose payments for political endorsements. Political groups and external actors also train influencers to push their messages, misleading voters into thinking their support is genuine.

Visit the Canadian Centre for Cyber Security website to learn more about cyber threats to elections. Here you will find information on how to protect your online data from cyber threats, as well as guidance for political parties, voters, election authorities and vendors to help mitigate the impacts of cyber threats to elections.

How do I know it’s disinformation?

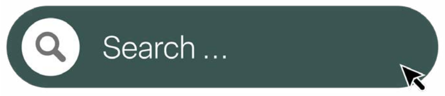
Be critical of what you see, read or hear. If you suspect that what you’re witnessing is disinformation, trust your gut and verify the information.

Use fact-checking tools

- Use fact-checking resources, like AFP-Canada, MediaSmarts fact search (bit.ly/fact-search), Les Décrypteurs (only in French) and Snopes.
- Include key words such as “hoax,” “scam,” or “fake” in your search.
- For more tips, check out Break the Fake.

Verify the source

- Use a search engine to see if the source exists and if they are credible.
- Use a reverse image search to make sure the image used is related to the story/current event.



Look at the design elements

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

✓ Canada
⊘ Canada

Validate domain names

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

✓ www.canada.ca
⊘ www.canada.net
⊘ www.canadaa.ca

Check other sources

- Check other sources to find out whether something fits with what most of the experts on that topic are saying.
- The News tab on Google is better than the main search bar.

What do I do if it’s disinformation?

Don’t share it. By simply not sharing it, you’re stopping its spread.

Report it. Social media platforms give users a way to report disinformation, and they will handle it from there.