Secure data and information

- encrypt sensitive data by using device and verified application encryption
- transport information securely using an encrypted USB or a secure storage container
- back up information regularly
- keep backups stored and encrypted offline to better protect against ransomware
- limit access accounts and information by practicing the principle of least privilege (for example, only authorized individuals can handle sensitive information)
- verify and validate messages and information before engaging and responding

Secure social media presence

- strengthen account settings to protect your personal information
- use fact-checking tools to validate sources before interacting with their content and platform
- review and sanitize content, images and videos to remove sensitive data before posting publicly
- restrict third-party app access to your social media profile
- educate your team on tips for spotting AI, deepfakes and disinformation
- avoid opening files and links contained in unsolicited text messages or emails
- report any suspicious activity to your IT security and security incident response team, if applicable

Secure online connections

- avoid connecting to public Wi-Fi where possible
- use cellular data or a secure Wi-Fi network to handle sensitive information
- change the default name and password of your router and Wi-Fi connection
- install Canadian Internet Registration Authority's (CIRA) Canadian Shield protective domain name service (DNS) on your router and personal devices
- confirm firewalls are enabled by checking the status in your device or system settings or with your service provider
- use only trusted mobile app stores and avoid unverified third-party apps

Secure staff and volunteers

keep staff members informed about current potential cyber threats and vulnerabilities

conduct awareness training to assist volunteers and new and existing staff to understand their roles and responsibilities

consider background checks for campaign staff and volunteers

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Cyber security advice for political candidates

Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security (Cyber Centre) is part of the Communications Security Establishment Canada. It is the single unified source of expert advice, guidance, services and support on cyber security for Canadians.

Canada

Why cyber security matters

Foreign cyber threat activity continues to target Canada's democratic process.

Threat actors target Canadian elections to influence decisions on key global issues or to exploit data and disrupt the democratic process.

Foreign threat actors can launch cyber attacks to disrupt election infrastructure, influence voters and spread disinformation. They can target political candidates by:

- hijacking accounts and online identities to spread false information
- disrupting campaign websites and infrastructure using distributed denial of service (DDoS) attacks
- hacking systems to leak sensitive (personal or campaign) data and embarrass, discredit or undermine a political candidate
- using ransomware attacks to disrupt campaign infrastructure and demand ransom payments
- creating content with artificial intelligence (AI), specifically generative AI, to spread disinformation

The following guidance includes cyber security measures to best secure your data, devices and online presence, and what preventative measures you should take to protect your assets and information.

How to secure your campaign

Consider the following security measures to protect your campaign from cyber threats:

Secure accounts

- use strong passwords and passphrases to all accounts
- avoid reusing passwords across accounts
- use multi-factor authentication (MFA) to add another line of defence against someone hijacking your account
- do not share access to accounts and systems unless necessary
- limit the use of "remember me" features on websites and mobile applications
- use a password manager to help create and secure credentials
- deactivate and remove accounts and profiles that are no longer in use
- regularly review your account security and recovery settings

Secure devices

- install anti-virus, anti-malware and anti-phishing software on devices
- secure access to your mobile device with a passcode or other forms of strong authentication
- update your devices' software, firmware and operating systems regularly
- enforce clear guidelines on handling campaign accounts and data on personal devices
- limit access to sensitive data on personal devices
- restart your devices regularly

For additional guidance and resources please see the Cyber Centre's guidance on cyber threats to elections.

cyber.gc.ca/en/guidance/cyber-threats-elections

Contact us
contact@cyber.gc.ca

Toll free
1-833-CYBER-88 (1-833-292-3788)

Media relations
media@cse-cst.gc.ca