Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

CYBER SECURITY ADVICE FOR POLITICAL CANDIDATES

INTRODUCTION

The Canadian Centre for Cyber Security has warned that foreign actors will likely try to interfere in Canadian election processes. If you're involved in politics – as a political candidate, staffer or volunteer – you are a target. It's vital that you take steps to protect yourself.

The Cyber Centre has advice to help you protect your cyber security and deal with threats to your social media accounts. The guidance in this brochure isn't all you need, but if you follow this advice, you can help make your campaign more cyber secure. For more extensive advice and guidance, visit cyber.gc.ca.

Cyber threat actors can target you:

- Directly through traditional hacking:
  - Hijacking social media accounts to discredit
  - Leaking campaign secrets/plans/internal communications
  - Blackmailing or embarrassing with sensitive information
- To discredit your campaign or platform:
  - Impersonation and parody accounts
  - Disinformation ("fake news")
  - Trolls/Bots
- As a target of opportunity, to gain:
  - Personal information
  - Financial details

You and your campaign are a target. Protect your campaign from a cyber security compromise and the complications that often accompany it.

Canada

PRACTICAL STEPS TO INCREASE YOUR CYBER SECURITY

Secure your campaign by taking these practical measures right now.

Use strong individual passphrases or passwords unique to every platform

Passphrases should be unique and passwords complex. Each account, website or device should have its own strong individual passphrase or password. Don't share your password. Only change your password when there's a good reason to do so, like if you think you've been compromised.

Enable Two-Factor Authentication (2FA)

Enabling a second factor of authentication (such as getting a text message with a code to allow you to log in) is another line of defence against someone hijacking your account.

Secure your mobile device with a passcode or other form of identification (fingerprint or face)

If your mobile device is lost or stolen, a lock code or other form of identification will be the only thing protecting your information. Plus, most devices automatically encrypt the information on them once you've enabled the PIN or passcode, further protecting your most sensitive information.

Regularly update (patch) your mobile devices and computer

Those updates include security patches. Don't ignore them.

Secure your social media and email accounts

Many people have a campaign manager or other dedicated support staff with access to their accounts. Know your options for delegating authority (what to do when you need multiple users to access one account). Use as many security options (settings) as you can for each social media platform.

Watch out for malicious messages

Phishing messages target a group of people by simulating a legitimate message from a trusted sender. Spear-phishing messages are tailored to you based on your work, your interests or personal characteristics. Be aware if the message seems out of character or off topic for the purported sender; call them to verify they sent it before opening. Never click on links or open attachments unless you are certain you know who sent them and why. If you don't know the sender, do not click.

Log out of accounts on shared desktop computers

If you log into any of your social media accounts on a shared computer, make sure you log out and never save your username and password. Don't access your account from untrusted devices like hotel business stations, which may be infected with malware.

Regularly review your account and recovery settings

Your social media and email accounts have a section for account recovery and password resets. Check them regularly to make sure they have up-to-date contact information and/or security questions. Make your privacy settings as high as possible.

Back up your information

Back up your campaign information in case you become a victim of ransomware. Know how to recover vital information if your device is damaged, lost or stolen.

Do not use free Wi-Fi

Free or unprotected Wi-Fi may be convenient, but it is relatively easy for anyone else on the network to eavesdrop. Don't access your email or social media accounts from free or unprotected Wi-Fi. If you choose to use free or unprotected Wi-Fi, do not type any sensitive information while you're connected. This includes login information for dedicated campaign sites.

CONTACT US

1-833-CYBER-88 or 613-949-7048

contact@cyber.gc.ca

cyber.gc.ca