KEEPING VIRTUAL EVENTS SECURE

As we keep stepping up our digital organizing to engage with even more Canadians, digital events and meet-ups are an important part of how we can stay connected and grow our movement.

Here are few important tips about how your video and teleconference events can be kept more secure:

✔ PROTECT YOUR ACCOUNTS

It's just as important to protect your log-in credentials for video and teleconference services as it is for email, social media, databases, or other networks.

- Use strong and unique passwords/passphrases, and don't share them with anyone.
- Enable two-factor authentication, which makes your account harder to access even if your password somehow gets compromised!

✔ PROTECT YOUR MEETINGS

You might have heard about 'Zoom-bombing.' It can happen to any video event or teleconference without the right safeguards, so don't let it happen to you!

- Ensure that all of your events and meetings are protected by a passcode / access code.
- Don't post event passcodes / access codes on social media, or anywhere except the intended audience. Even open engagement events can be disrupted by party crashers of any kind.
- Avoid using personal meeting codes for public meetings.
- Use 'waiting rooms' or similar tools where possible to ensure others can't speak before the host, or that uninvited users aren't automatically admitted.
- You can also "mute participants on entry," particularly for large groups.

✔ PROTECT YOUR COMPUTER OR DEVICE

Watch what you download.

- When possible, use web-based apps for video and teleconferencing services
- As always, watch the links you click! Services like GoToMeeting, Zoom, Google, Webex, and many others have all had attempts by bad actors to impersonate their domains or what their apps look like, so avoid malware by making sure you're only downloading the correct app.
- Install the latest updates to keep your devices and apps as secure as possible.

✔ PROTECT YOURSELF

Is this recording??

- Always adjust settings to be aware of whether your camera or microphone or on, and to ensure your screen (or the calls you set up) aren't being unintentionally recorded.
- Don't use video or teleconferences for sensitive discussions, and don't assume these communications are end-to-end encrypted.
- In a way, video calls often mean inviting others into your home. Make sure you're in the appropriate setting, and that you aren't including shots of your family or personal living spaces that you don't want the world to be seeing. That also means making sure your background is clear of wi-fi passwords or other private or professional information.
- The mute button is your friend — *toilet flushes can really send a call swirling!*

➡ LEARN MORE ABOUT STAYING CYBER-HEALTHY DURING COVID-19, AND ALWAYS:

The Canadian Centre for Cyber Security has a variety of resources to help you stay cyber-secure, and you find those here: cyber.gc.ca/en/guidance/staying-cyber-healthy-during-covid-19

For more information, contact **it-ti@liberal.ca**