Zoom Meeting Tips and Reminders from the BCSA Executive

Since our gatherings were forced online by the pandemic last spring, many of us have regularly used *Zoom* meetings for teaching and for most presentations and gatherings.

A ***Zoom* meeting** is a relatively open platform for gathering with the potential for interaction and collaboration. A ***Zoom* webinar** requires a different level of account and is a presentation platform—attendees are not heard or shown on the screen. A detailed comparison of the two formats can be found *here*.

As we all know by now, the shift to *Zoom* has provided new opportunities for people to anonymously enter and disrupt particular gatherings, an act widely referred to as *Zoombombing*. Racist, misogynist, homophobic, xenophobic trolls have especially welcomed the opportunity to attack and indeed terrorize gatherings of predominantly Black, Indigenous, queer and / or disabled people. There are many, *many* examples of such incidents reported online. We will not cite and shine light on specific examples here, lest we feed the cowardly perpetrators with attention or further the reach of their assaults.

Several of our members have had such negative and harmful experiences online, and so as we enter the winter semester and approach a full year online, we offer the following tips and reminders about hosting and participating in *Zoom* meetings.

Please note that ***Eventbrite* will not save you.** Requiring registration is one way to track interest and likely participants; it can help control who enters the meeting if registration lists are consulted as admission is granted. Registration can help to protect links to *Zoom* meetings, however, even if only registered participants receive the link to a meeting, people register for events under fake names and email addresses and share links all the time.

Under Security settings, **enabling the waiting room prior to an event** is often understood as a first line of defense. It can allow for a host to compare waiting attendees to a registration list and admit them into the event accordingly.

You might choose to "**Hide profile pictures**" under security settings, which will show participants in the room by username rather than allowing the use of profile pictures.

Under the "Participants" tab, select "**Mute All**" to prevent audio interruptions.

Under "Screen Share" tab, select "**One participant can share screen at a time**" to prevent overlaying of screen images.

Returning to the Security settings, there is a list of **options to control how participants can take part in a meeting**. Zoom bombers exploit these options as they are available to them:

- To discourage anonymity, do not allow participants to **rename themselves**. One trick of *Zoombomber*s is to switch identities during an attack to avoid detection and remain in the room to pursue subsequent rounds of attack.
- To prevent potential audio interruptions: do not allow participants to **unmute themselves**.
- To prevent potential visual interruptions: do not allow participants to **share screen**; you may also choose not to allow participants to **start video**
- To prevent text interruptions: do not allow participants to **access chat**.

Zoombombers often test out their access before launching an attack. They may begin with a seemingly innocuous interruption or chat comment that could go unnoticed or create momentary confusion. This can confirm that a meeting is vulnerable give the cowards the go ahead.

It can be very helpful to have co-hosts of a meeting whose primary role is to monitor participants throughout the event, look out for suspicious activity and identify and remove any participant/s who act in a harmful manner.

The goal must be to prevent harm. If you have chosen to grant participants interactive access and a strange or unexpected visual or audio occurs, we recommend immediately shutting down participant access. If a legitimate participant has made a mistake you can always readjust the settings. Acting fast can stop an incident, so better to be too cautious than not cautious enough! We encourage those who care for children attending school online to remind them regularly that if anything seems weird or scary to close their computer right away and tell you or an adult they trust.

Although these measures are important and necessary, preventing *Zoombombing* does not begin nor end with these increased measures; it must also include interventions that disrupt the present climate and environment that supports these types of harmful behaviours. We urge our non-Black and non-Indigenous colleagues and community members to engage in open dialogues with their students, colleagues and communities regarding the tenets of *Zoombombing* and the climate in which it exists. How are you able to disrupt the behaviour and vigorously reject continuing passive support? The strategies for preventing *Zoombombing* that we have outlined here are only part of the process.

It is one thing to know that *Zoombombing* exists, and quite another to experience it first-hand. Please protect yourselves and the participants in your meetings from attacks and their lasting reverberations. If you ever are attacked and feel you have lost control of the online space, it is best to make an announcement and end the Zoom meeting altogether to prevent further harm. **There is no academic gathering more important than your well-being—we keep us safe.**

With love and care from the BCSA Executive