Dear Colleagues,

I am sending a reminder to all faculty and staff on security considerations for zoom users at Queen's University.

The following steps are recommended to protect your meetings:

1.**PASSWORD PROTECT YOUR MEETINGS**
The simplest way to prevent unwanted attendees and hijacking is to set a password for your meeting. Passwords can be set at the individual meeting, user, group, or account level for all sessions. In order to do so, first sign in with your account at the Zoom web portal. If you want to set up a password at the individual meeting level, head straight over to the "Settings" tab and enable "Require a password when scheduling new meetings", which will ensure a password will be generated when a meeting is scheduled. All participants require the password to join the meeting. Subscription holders can also choose to go into "Group Management" to require that everyone follows the same password practices.

2. **AUTHENTICATE USERS**
When creating a new event, you should choose to only allow signed-in users to participate.

3. **JOIN BEFORE HOST**
Do not allow others to join a meeting before you, as the host, have arrived. You can enforce this setting for a group under "Account Settings."

4. **LOCK DOWN YOUR MEETING**
Once a session has begun, head over to the "Manage Participants" tab, click "More," and choose to "lock" your meeting as soon as every expected participant has arrived. This will prevent others from joining even if meeting IDs or access details have been leaked.

5. **TURN OFF PARTICIPANT SCREEN SHARING**
No-one wants to see pornographic material shared by a Zoom bomber, and so disabling the ability for meeting attendees to share their screens is worthwhile. This option can be accessed from the new "Security" tab in active sessions.

6. **USE A RANDOMLY-GENERATED ID**
You should not use your personal meeting ID if possible, as this could pave the way for pranksters or attackers that know it to disrupt online sessions. Instead, choose a randomly generated ID for meetings when creating a new event. In addition, you should not share your personal ID publicly.

7. **USE WAITING ROOMS**
The Waiting Room feature is a way to screen participants before they are allowed to enter a meeting. While legitimately useful for purposes including interviews or virtual office hours, this also gives hosts greater control over session security.

8. **AVOID FILE SHARING**
Be careful with the file-sharing feature of meetings, especially if users that you don't recognize are sending content across, as it may be malicious. Instead, share material using a trusted service such as Box or Google Drive. At the time of writing, Zoom has disabled this feature anyway due to a "potential security vulnerability."

9. **REMOVE NUISANCE ATTENDEES**
   If you find that someone is disrupting a meeting, you can kick them out under the "Participants" tab. Hover over the name, click "More," and remove them. You can also make sure they cannot rejoin by disabling "Allow Removed Participants to Rejoin" under the "Settings: Meetings - Basic" tab.

10. **CHECK FOR UPDATES**
    As security issues crop up and patches are deployed or functions are disabled, you should make sure you have the latest build. In order to check, open the desktop application, click on your profile in the top-right, and select "Check for updates."

For more information, please see https://www.queensu.ca/its/zoom/security-considerations-zoom-queens. If you need help with this, you can ask and the IT Support Centre will walk you through it (613-533-6666).

If your meeting is “bombed,” it is recommended that you either:

1) Turn off participant microphone & screen sharing and then remove participant

OR

2) End the meeting immediately

There is an attached document on Best Practices for Securing Your Zoom Meetings and a PowerPoint slide that you can circulate to your teams for them to share in your meetings to inform, and to remind, of the importance of securing all online meetings.

Please contact your Head of Department and copy deanartsci@queensu.ca with any security issues or concerns.

Regards,

Barbara Crow

Barbara Crow, PhD
Dean, Faculty Arts & Science
Queen's University
Kingston, ON Canada K7L 3N6
bc100@queensu.ca
Tel 613 533-2446
http://www.queensu.ca/artsci/
Ageing, Communication and Technologies, http://actproject.ca

Queen's University is situated on traditional Anishinaabe and Haudenosaunee Territory.