As schools adjust to the COVID-19 pandemic, many have shifted to communicating remotely using video conference platforms like Zoom, prompting a hacking phenomenon known as “Zoom-bombing.” In a typical attack, an unwanted perpetrator tries to disrupt an online class by hacking in and displaying images and language that may be pornographic, hateful or threatening in nature.


The New York Times published an article outlining Zoom Security Tips – although the article is specific to the Zoom platform these tips can likely be applied to many video conference systems:

- Don’t share your Zoom link or code on social media – as anyone who has the link can join the meeting.
- Set a meeting password
- Create a waiting room
- Set screen sharing to “host only”
- Turn off the annotation feature
- Make sure you’re running the latest version of Zoom
- Restrict other features as needed in host controls:
  - Block private chat
  - Disable “join Before Host” so no one can’t cause trouble beforehand.
  - Disable “File Transfer” this will prevent digital virus sharing.
  - Disable “Allow Removed Participants to Rejoin” that way “botted” attendees can’t slip back in.
OSBIE recommends researching any platform you are using and to apply as many security features as possible to prevent your next online class from being Zoom-bombed!

Obtain direction from your school board's IT resources on approved platforms to use including how to enable any applicable security settings.

Do you have a topic you'd like featured in OSBIE’s risk management blog? We’d love to hear from you, please email us at rm@osbie.on.ca.

***