

Dear NOBCChE Member,

We hope that you have had a strong start to 2021 and have a productive year planned. With the world moving further and further into a virtual environment, NOBCChE Leadership wants you to be safe and to be able to host events without concern for virtual safety.

Recently, a NOBCChE chapter was “Zoom Bombed” with slurs and derogatory speech. We are working with the proper authorities to identify the culprits. In the meantime, we are sharing some tips with our NOCChE members to reduce the risk of this happening again and assist in keeping your zoom sessions safe.

- 1) *Don't share Zoom information freely on social media.* When making flyers for social media advertisement, it's best to include a contact email for the chapter and then, add the persons interested to a mailing list, so Zoom information is circulated through a more controlled channel.
- 2) *Set a waiting room.* With a waiting room enabled, hosts can control who enters and who has access to controls within the meeting. This way, only those who are associated with the event can be admitted by the meeting host.
- 3) *Don't use personal meeting IDs for public events.* A personal ID is the default for when you launch zoom and start your meeting. With access to this, someone could potentially join your Zoom sessions, scheduled or not.
- 4) *Require a passcode.* When creating your zoom meeting, setting a passcode is a great first line of defense for the meeting room itself. When creating advertisements, do not put the passcode in the flyer or advertisement until closer to the time of the event to limit sharing of the passcode.
- 5) *Only allow registered users (optional).* When only registered users are allowed to join the event, users must have an account through Zoom and in some cases through an email from the license holding institution to join the meeting. This can be used to restrict entering attendees. (ex: nobcche.org emails would be the only groups admitted to a registered zoom meeting launched through a nobcche.org licensed zoom account.)

We hope that these tips help keep our members safe in this increasingly virtual world in which we reside. Please contact your university or institution's IT department to get more assistance with Zoom or other supported virtual meeting platform security and safety procedures.

Stay Strong,

NOBCChE Executive Board (Student Representative, Regional Chairs, & Officers)