Securing Zoom Meetings: Preventing “Zoom Bombing”

Many of us are using Zoom extensively as we teach and work remotely. This is true not only at NMU, but nationwide. As the popularity of Zoom has grown, so has the temptation for hackers to maliciously enter and disrupt Zoom meetings. The technology media has nicknamed this practice "Zoom Bombing." Unfortunately, NMU has not completely avoided the Zoom Bombers, though with proper security options enabled it can be minimized.

How does it Happen?

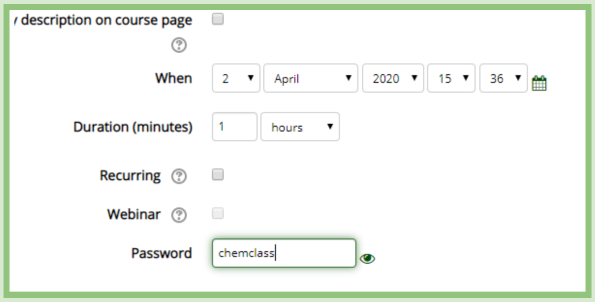
It may be helpful to understand how the hackers make these intrusions. They are **not** targeting a specific meeting or institution, such as starting with the objective of disrupting a 3pm English course at NMU.

What they are doing is generating URLs (web addresses) or meeting codes that follow the structure that Zoom uses, then testing to see which of those codes actually connect them to any Zoom meetings. When they get lucky and generate a code for an actual meeting, they enter it and disrupt it by posting rude comments in the chat, doing inappropriate things on video, etc.

How Can We Prevent It?

Fortunately, there are some easy things we can do to prevent this from happening. Probably the simplest thing is to assign your Zoom meeting a password that you provide to your participants.

Setting a password can be done through EduCat when you create meetings there, or through Zoom's interface if you are logging in directly to Zoom to create your meeting. Even if a hacker generates a URL that matches your meeting, they won't know your password and so will not be able to enter. Unlike most passwords, this doesn't necessarily have to be complex, but does have to be 6 characters or more.



/ description on course page ☐

When 2 April 2020 15 36

Duration (minutes) 1 hours

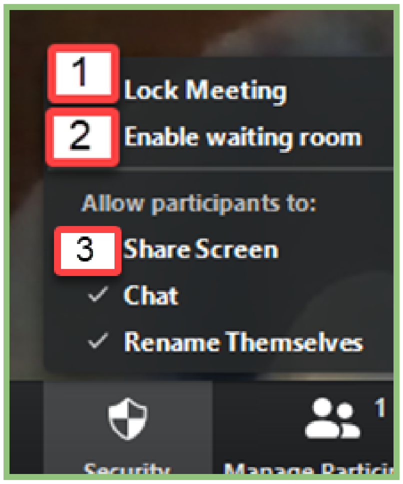
Recurring ☐

Webinar ☐

Password chemclass

Note: As of Winter 2021 security features are built into the creation of every new Zoom meeting. If you don’t create a passcode the room will default to using the Waiting Room.

Security Options located at the bottom left of your Zoom window alo gives us a few more security measures to choose from.



1. **Lock Meeting** allows you to lock your room after the meeting begins, once all your expected attendees are present. One possible issue with this method is that people who are late to the meeting will not be able to get in, and someone who loses their connection will not be able to re-enter.

2. **Enable waiting room** makes it so the meeting host receives a notification each time someone tries to enter the meeting, and can choose whether to admit them or not. This cannot currently be enabled through EduCat, but can be turned on through the **Zoom site**.

3. Another precaution that Zoom has taken is turning off screen sharing for participants by default. That way if someone does make it into the room who isn't welcome, they won't be able to hijack the screen. You can enable **ShareScreen** for your participants under the security options as well.

Additional Information:

You may also be interested in reading "Best Practices for Securing Your Virtual Classroom," on Zoom's user blog.

Questions?

If you have questions about using Zoom for your classes, please contact us at the Center for Teaching and Learning, ctl@nmu.edu or 227-2483.
For general Zoom questions, you can also contact **Audio Visual Services at 227-2290 or av@nmu.edu.**