HOW TO PREVENT ZOOMBOMBING

Presented by UNT Student Activities
WHAT IS ZOOMBOMBING?

Zoombombing is a method of trolling in which hackers disrupt zoom meetings with disturbing videos, pictures, and statements. Most Zoom meetings have a public link that, if a person were to click it, it will allow them to join. Therefore, it is very easy to do and can cause many forms of disruption.
**Tips to Prevent Zoombombing**

**Do not share link**
Don’t tweet, facebook, or insta post your zoom link publicly. This is the easiest gateway for zoombombers!

**Use a password**
Go to your zoom settings to set up a password for people joining your meeting.

**Lock the meeting**
After everyone has arrived, go to manage participants, click on more, and choose to lock the meeting. It’s always a safe option!

**Disable personal ID**
Zoombombers can trace all of your meetings if you share your personal ID. To set up a random meeting ID, go to settings and click on the meeting tab.

**Kick people out**
The easiest way to get rid of the trolls is to kick them out. Go to the participants menu, the person’s name, and then select to remove them.

**Assign co-hosts**
For extra security, assign a co-host by clicking on the three dots that appear on the participant’s webcam.
ADDITIONAL TIPS

BEFORE MEETING:

- Disable auto saving chat
- Disable file transfer
- Disable screen sharing for non-hosts
- Disable remote control
- Disable annotations
- Use per-meeting ID, not personal ID
- Disable "join before host"
- Enable "waiting room"

DURING MEETING:

- Assign at least two co-hosts
- Mute all participants
- Lock the meeting, if all attendees are present
To learn more, visit:
https://www.adl.org/blog/how-to-prevent-zoombombing

Connect with us!

@UNTactivities @UNTactivities @UNTactivities