How to Avoid Zoombombing

We know many of you are seeing [articles](https://www.cnn.com/2020/04/02/us/fbi-warning-zoombombing-trnd/index.html) and Facebook posts about “Zoombombing.”   Zoombombing is a form of cyber harassment where someone hijacks a Zoom session, often sharing threatening, violent, or pornographic images and messages.  Zoom is one of the more popular web chat technologies, but, fortunately, it is not the web conferencing technology that we are primarily using here at New Paltz.  Although any web conferencing tool could succumb to cyber harassment, we are not seeing the same level of abuse with WebEx or with Blackboard Collaborate.  In general, your Blackboard Collaborate Ultra Rooms will be safe since participants are likely to enter through their Bb class rather than through an email invitation link.  Still, you may want to take precautions to increase the security of your web conferencing sessions.  See this Zoom blog, [How to Keep Uninvited Guests Out of Your Zoom Event](https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/).  If you are using Zoom for work or for social connection during COVID 19, we recommend that you take these practical steps to avoid having your session hijacked.  Similar principles apply to other web conferencing tools:

* Avoid sharing your meeting link in any public forum or social media site unless you really want to make it available to anyone.
* Avoid using your Personal Meeting ID to host any truly public events.
* Use features, such as Zoom’s Waiting Room, to lock your meeting, allow only signed-in users to join, or otherwise control who can come in and exit your web conference.
* Unless it is important for others on the call to share their screens with the group, do not select features that allow someone other than you (the host) to screen share.