**ZOOM Meetings**

There a few disturbing things taking place on the Zoom platform that you need to be made aware of.  Video hijacking or (Zoom Bombing) attempts occur when conferences are hosted on public channels shared over the internet via URLs, making them accessible to anyone.  Someone can gain access to your meeting and use inappropriate language or use your screen share to place items on the screen that may be inappropriate for your class.

However, there are several things that we can do to prevent this from happening. You can use one or a combination of preventions to make sure that you will not experience any Zoom bombing.

1.  Require a meeting password
You can protect your meeting by using a password.

2.  Require a meeting password
You can also enable ‘Embed password in meeting link for one-click join.’ This prevents an actor from accessing your meeting without losing the usability of sharing a link to join.

3.  Allow only hosts to share their screen
Go into your settings and make sure that only the host can share information to the screen. This will prevent any outside disruption from the main video feed on a public session.  Don’t let anyone hijack the screen during a Zoom call. To prevent it, make sure your settings indicate that the only people allowed to share their screens are hosts. Navigate to Personal > Settings > In Meeting (Basic) and look for Screen sharing. Check the option that only allows the host to share.

4.  Use a unique ID for large or public Zoom calls
Use a unique ID and not your personal meeting ID. This allows a one-time code and prevents hijackers or bombers from jumping in on your Zoom meetings at any time using your personal meeting ID.

5.  Don’t share the unique ID publicly
Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific meeting attendees.

6.  Create a waiting room
When participants log into the call, they see a Waiting Room screen that you can customize. They aren’t let into the call until you, the host, lets them in. Hosts allow people in all at once or one at a time, This lets you screen the attendees and if you see names you don’t recognize in the Waiting Room, you don’t have to let them in at all. Click on Managing Participants at the bottom of your screen, click on more, and click on put participant in waiting room on entry.

7.  Lock a meeting once it starts
If you start a meeting and all attendees have joined, hosts can lock the meeting from new participants. During the session, navigate to the bottom of the screen and click Manage Participants. The Participants panel will open. At the bottom, choose More > Lock Meeting.

8.  Remove attendees or put them on hold
Hosts can kick unruly attendees out of a call or put them on hold. To remove an attendee, hover over the name of the person you want to remove on the Participants panel on the right. When options appear, choose Remove. By default, an ousted guest cannot rejoin. To put the guest on hold: During the call, find the video thumbnail of the person you want to put on hold. Click on their video image and select Start Attendee On Hold. Hosts can reverse this action by clicking Take Off Hold in the Participants panel.

9.  Disable the participant’s camera
Hosts can turn off any participant’s camera by opening the Participants panel and clicking on the video camera icon next to the person’s name.

10.  Keep Disable File Transfer settings active
Keep default settings on to Disable File Transfer to limit participants from sharing files, including images and animated GIFs within the chat. Open Settings in the Zoom web app (it’s not in the desktop app). On the left side, go to Personal > Settings. Then click In Meeting (Basic). Scroll down until you see File Transfer and slide the toggle to disable.