Dealing with Zoom-bombing

Risks:

1. Screen sharing inappropriate content
2. Inappropriate content on video camera
3. Inappropriate sound via audio
4. Inappropriate names and/or pronouns
5. Inappropriate profile photos
6. Inappropriate chat messages
7. Inappropriate direct messages to other participants
8. Inappropriate files posted in chat

Precautionary measures:

1. Non-impactful
    a. Lock down non-essential features.
        i. Whiteboard
        ii. Notes
        iii. AI
    b. Screen share - host and co-host only.
    c. Turn off file sharing.
    d. Turn off annotations.
2. Impactful
    a. Disable profile pictures.
    b. Restrict Chat.
        i. Suggest meeting business only.
    c. Restrict renaming.
        i. Host reviews names upon entry and during the meeting.
    d. Require authentication
        i. People must sign into their zoom account before joining.
            - Provides traceability for participant actions, which discourages malicious behavior, because actors can be reported to Zoom.
    e. Implement waiting room.
        i. Host must admit participants – may be cumbersome.
            - Provides a buffer between the meeting and a bad actor - a proactive review by the host and immediate recognition of a newcomer and potential bad actor.

Response to an incident

1. Click **Host Tools** >>> **Suspend All Participant Activities** >>> **Suspend** (leave **Report to Zoom** *checked*)
    a. Immediately stops problem.
    b. Participants are all put in the waiting room.
2. Host should ***announce verbally that the meeting has been temporarily suspended*** due to inappropriate activity.
    a. After suspending all participant activities, participants will be able to hear the host, but other attendees will all be muted.
3. Address bad actor.
    a. Remove from meeting and block.
4. Re-admit others.
5. Re-enable other features
    a. Allow unmute, etc.