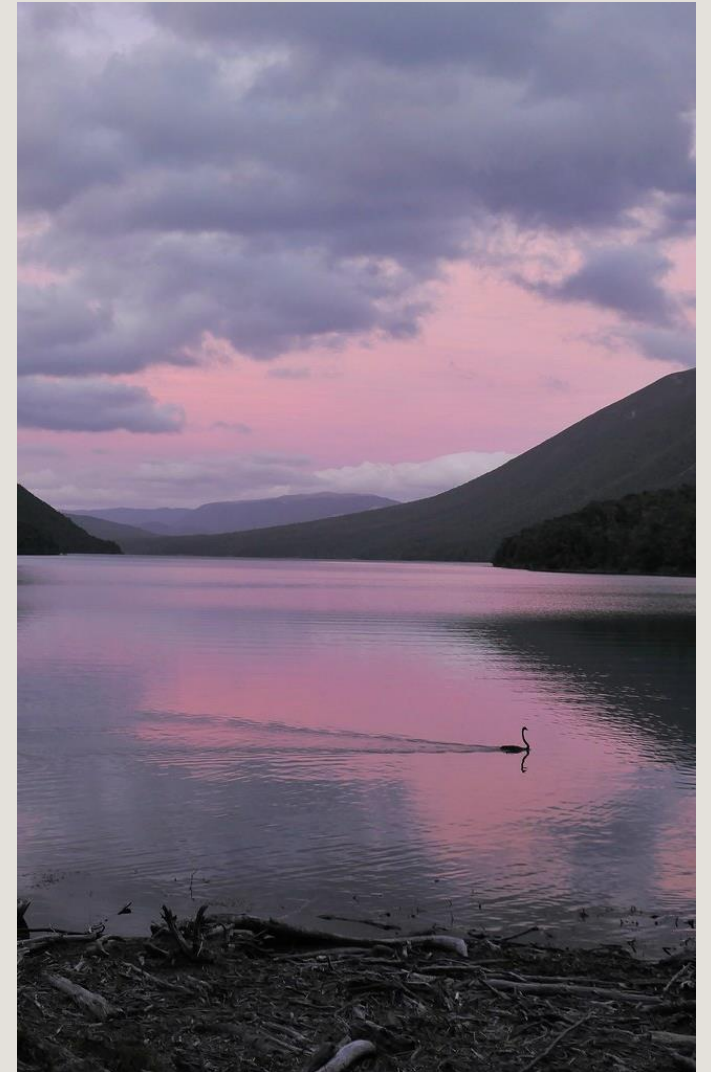


# MAKING YOUR ZOOM MEETING SECURE

---

OA Region 8 Technology Committee



[This Photo](#) by Unknown Author  
is licensed under [CC BY](#)

# Agenda

WHY WE NEED SECURITY

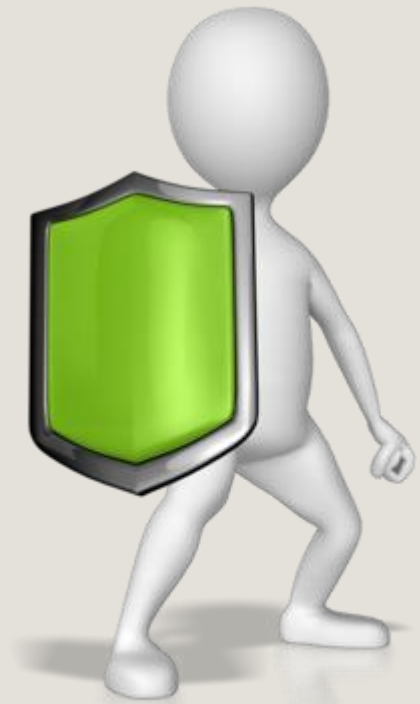
WHO CAN PROVIDE SECURITY

HOW TO BECOME A HOST/COHOST

SECURITY SETTINGS

WHAT TO DO IF YOU HAVE AN INTRUDER

BEWARE OF THEIR TRICKS



This Photo by Unknown Author is licensed under [CC BY-SA-NC](#)

# WHY WE NEED SECURITY

Security: Is the state of being free from danger or threat

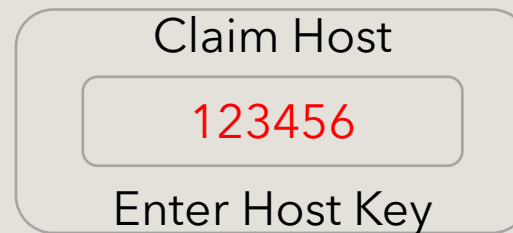
It is important OA members feel safe to share their experience, strength, and hope. The goal of security is to prevent people from intruding upon and disrupting the meeting with various means of shock.

**REMEMBER THESE PEOPLE DO NOT KNOW YOU. TRY NOT TO TAKE THEIR ACTIONS AND WORDS PERSONALLY.**

# WHO CAN PROVIDE SECURITY TO THE MEETING

Any member of the OA group with the **HOST KEY** can assume the **host position** by entering the 6 digit host key 2 ways.

1. Click on the box **Claim Host** before entering the meeting. Type in the **Host Key**
2. Once in the meeting go to **Participants**. Go to the 3 dots ... lower right-hand corner select **Claim host**, enter the **Host Key**

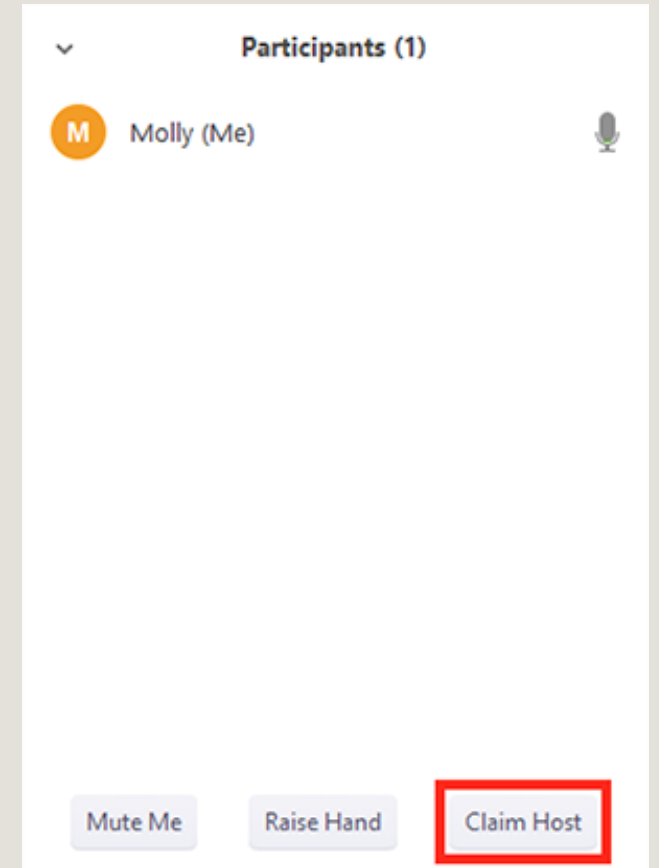


Claim Host

123456

Enter Host Key

3. Some Zoom accounts have security settings to only open the meeting with a Host first signing into the Zoom account with a user name and password.



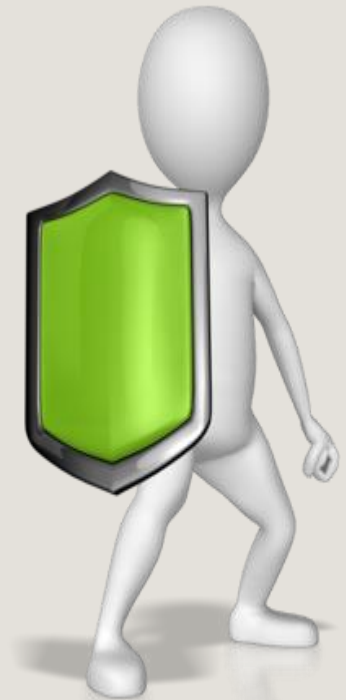
# WHO CAN PROVIDE SECURITY TO THE MEETING

The **HOST KEY** is a numeric code which allows someone to claim the host role during a meeting. It is the most important part of the security process. Only provide the host key to members who are regular attendees and have the understanding of how to use it.

There are many resources online that provide training if you have a desire to learn. The San Francisco OA Intergroup holds regular online trainings to reach Zoom security.

Ideally, each virtual meeting has at least 2 or 3 members who can provide security for their meeting as a team.

One person is the host and the others may be cohosts, assisting security by monitoring the waiting room, the mute key, and other security measures.



This Photo by Unknown Author is licensed under [CC BY-SA-NC](#)

# Security Settings

1. Click on the Shield on bottom of screen
2. Select your Preferences

On this screen you can select what you want to allow or restrict.

**Lock Meeting:** You can lock the meeting down. No other members may enter.

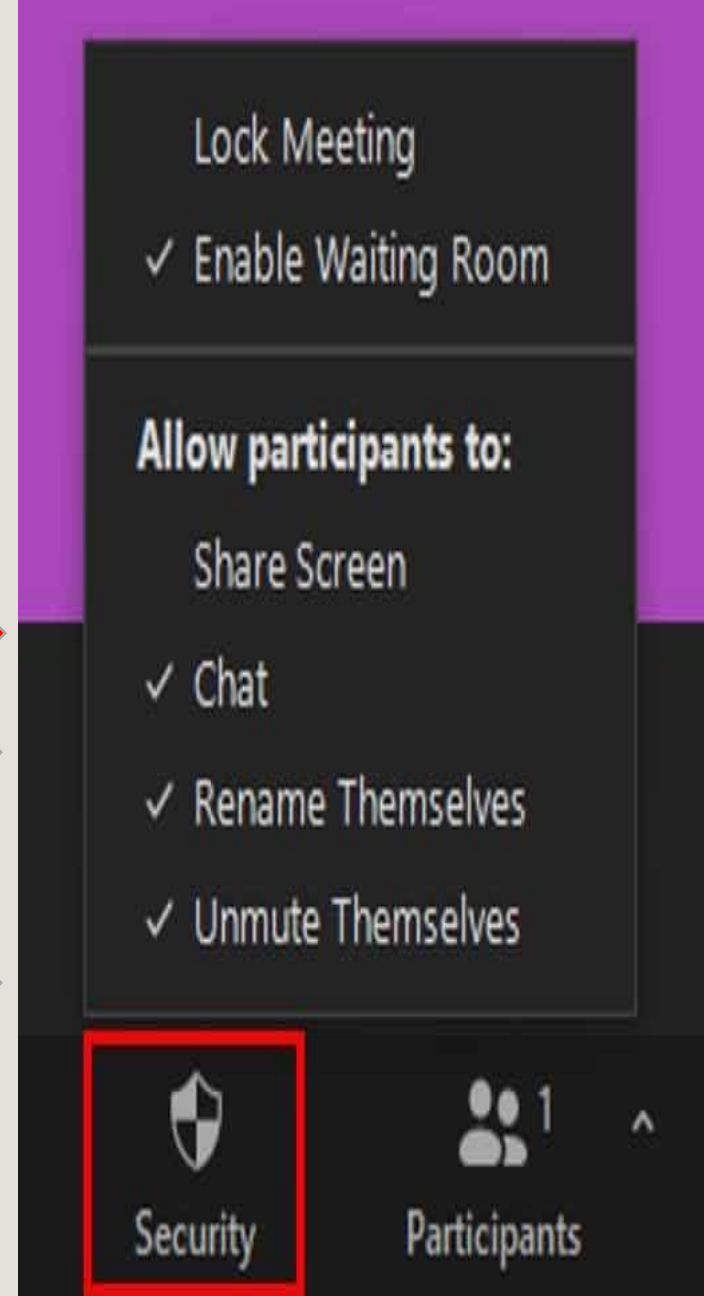
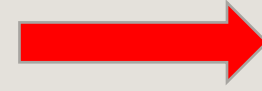
**Enable Waiting Room:** Participants enter a waiting area and are held until let in by host/cohost. Host/cohost may click on someone in participants and send them to the waiting room.

**Share Screen:** If you click this it will allow intruders to screen share anything on screen. It is more secure to not enable this.

**Chat:** You may limit participants ability to chat. Intruders may place obscene messages in chat. Some meetings chose to enable chat later during the meeting.

**Rename themselves:** Participants may rename themselves.

**Unmute themselves:** If you have a cohost to mute and unmute participants as they raise their hand to share, you may chose to limit participants ability to unmute themselves.



# Participants Settings

On this screen you can select what you want to allow or direct. Click on **More**

**Ask to start video:** Participants will get a notice on their screen to turn on their video.

**Make host:** You can assign host and cohost to other participants.

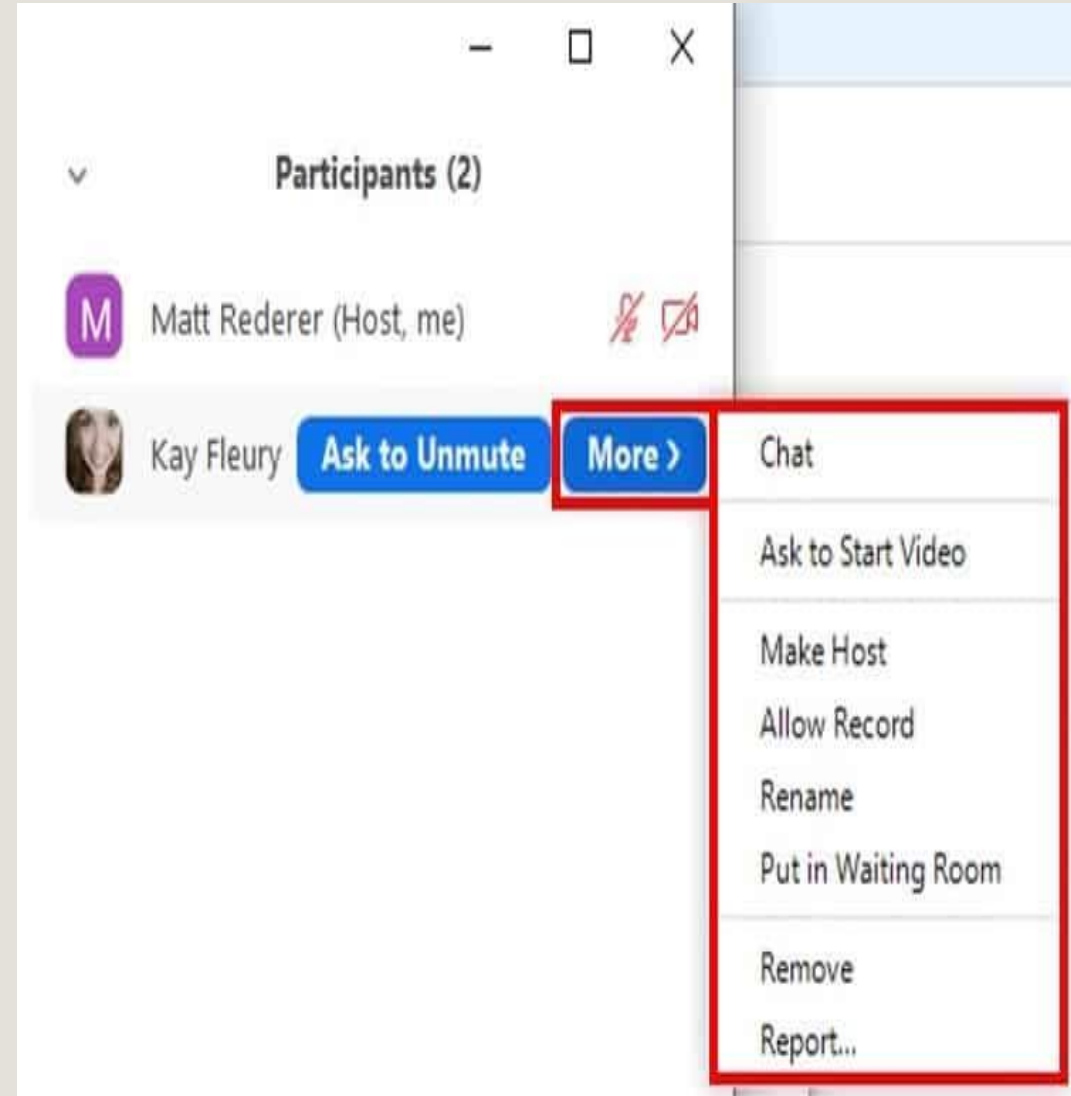
**Allow to record:** rarely used because of anonymity.

**Rename:** Allows participant to rename themselves.

**Put in waiting Room** You may place a disruptive participant in the waiting room.

**Remove:** Removes the person from the meeting. They won't be able to rejoin unless you allow participants to rejoin.

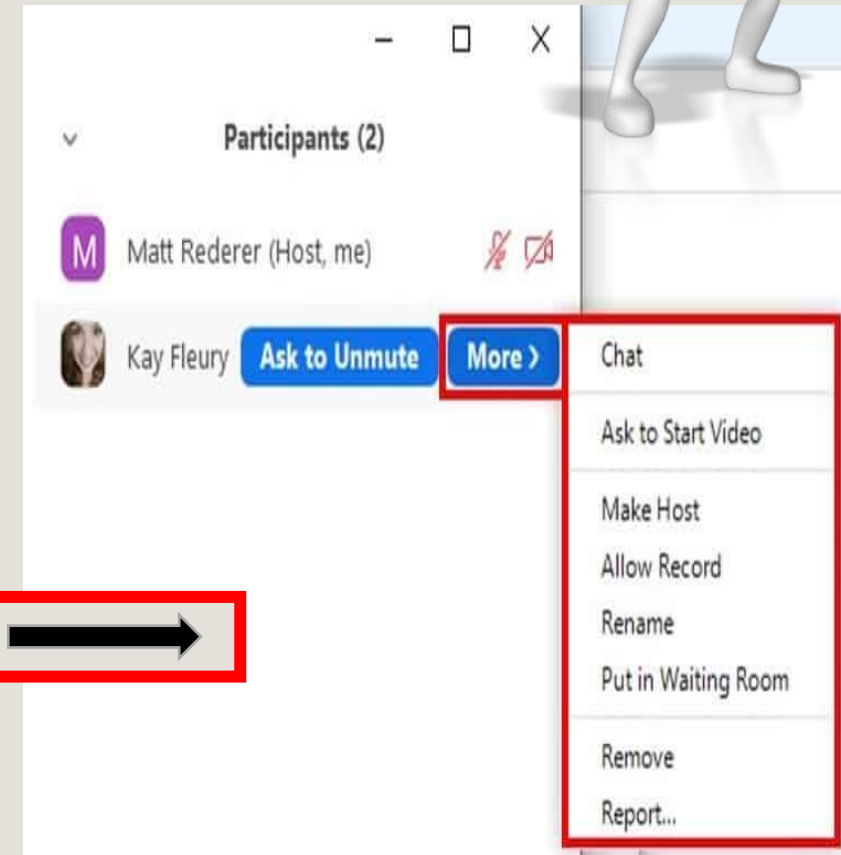
**Report:** Send a disruptive participant's information to Zoom Support.



# WHAT TO DO IF YOU HAVE AN INTRUDER

## First don't panic

1. Identify the intruders. Remember their cube will light up around the participants who are currently sharing.
2. The host/cohost may remove the intruder(s) from meeting or move them to the waiting room.
3. Do not engage with the intruder. Keep your focus on putting them in the waiting room.
4. Usually intruders will attend a meeting with other intruders who act as a team.



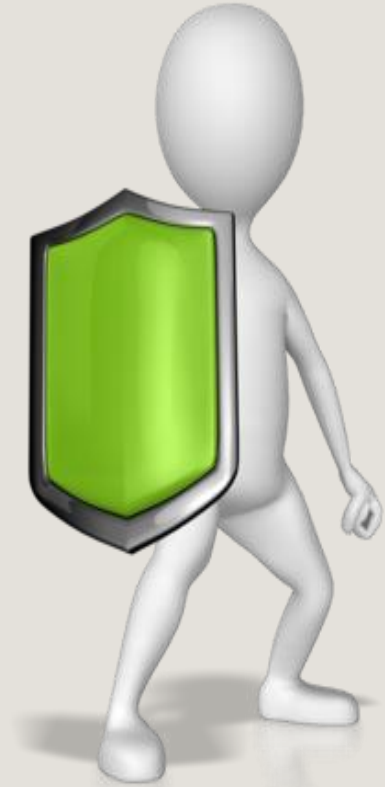


# WATCH FOR INTRUDER TRICKS

1. **BEWARE** of people asking for the host key. Never give it to an unknown participant. Avoid deep fakes by always verifying even members who you know. Deep Fakes are intruders posing as regular attendee by displaying a manipulated moving image of that regular attendee. Ask the participant to prove they are not a deep fake by physically raising their hands on the video or answer a question only an OA member would know.

**Example questions:** Who is the OA founder? or Name the principle of step one.

1. Deep Fakes may use Artificial Intelligent (AI). They capture a known image and or audio to impersonate a member.
2. When participants are able to share screen, intruders may project obscene photos or draw on the white board.
3. Intruders may also leave obscene messages in the chat.



# **OVEREATERS ANONYMOUS®**

Region 8

