ZOOM QUICK TIPS

Privacy & Security

COASTLINE COLLEGE

CYBER CENTER

SECURE YOUR MEETING

GENERATE MEETING ID

Never use your personal meeting ID

CREATE A PASSWORD

Always use a meeting password and share it securely

WAITING ROOM

Use Zoom's waiting room feature to approve guests

DISABLE AUDIO & VIDEO

Mute audio & disable video for meeting participants

SAFE LINK

Do not share your meeting link on social media or websites

HOST-ONLY SCREEN SHARE

Turn off screensharing for everyone except the meeting host

MEETING LOCK

Lock the meeting after it starts

ZOOM UPDATES

Install Zoom application updates

SECURITY & PRIVACY

INTERNAL MEETING

- Never use your personal meeting ID
- Do not share your meeting link on social media or websites
- Always use a meeting password & share it securely
- Mute audio for all participants upon entry to the meeting
- Turn off screensharing for everyone except the meeting host/co-host
- Lock the meeting after expected participants have joined

VS

EXTERNAL MEETING

- Never use your personal meeting ID
- Do not share your meeting link on social media or \websites
- Use Zoom's waiting room feature
- Mute audio and disable video for meeting participants
- Do not check Enable join before host
- Turn off screensharing for everyone except the meeting host/co-host
- Disable private chat sessions
- Lock the meeting after the meeting starts to prevent late party-crashers
- Turn off file transfer & annotations
- Record the meeting in the cloud

BOOT THE PARTY-CRASHER

Kick unwanted guests out of your meeting by selecting “Remove” in the Participants menu

Lock the meeting to prevent the party-crasher from returning

RISKS & CONCERNS

Zoombombers, trolls, and party-crashers have the worst intentions to disrupt your meeting and push unwanted material or hate messages. Be aware of the risks and concerns, keep your meetings free of the propaganda that cyber attackers try to push, and learn about Zoom's features that can prevent attackers from entering your meeting.

PRIVACY & REGULATORY CONCERNS

PERSONAL INFO

CONFIDENTIAL INFO

SENSITIVE INFO

ZOOMBOMBERS, TROLLS, & PARTY-CRASHERS

- Participants can share confidential information in the meeting chat (the chat is not private, it is stored to the Zoom servers and the meeting host gets a copy after the meeting)
- Participants can display unwanted images or content in their profile picture, video, screensharing, annotations, file-sharing, chat, or private chat
- Zoom has the right to use your personal data, according to Zoom's privacy policy
- Participants can share your meeting invite publicly
- Party-crashers can join your meeting through war-dialing (guessing the meeting ID)

+ Add unwanted images in the file-share feature
+ Add unwanted messages in the chat box
+ Post phishing links in the chat box
+ Can scream obscenities into the microphone
+ Share unwanted images or video using the video feature
+ Share unwanted images using the profile picture
+ Can return to the meeting using another participant ID

Tobi West, CISSP, GCFE
Professor, Cybersecurity
Coastline College Cyber Center