ZOOM TIPS

With Zoom gaining popularity as one of the top work-from-home and K-12 online meeting tools for the pandemic-era, the community has seen an increase in Zoom-bombers, trolls, and party-crashers. We want to provide a safe environment for our meeting participants, regardless of their age or affiliation with our organization. Keep in mind that Zoom was initially developed to be user-friendly and convenient, connecting people inside and outside of our organization with a simple click on a meeting link. Zoom did not initially focus on security or privacy to prevent malicious attacks during online meetings where school teachers are meeting with young students or co-workers are meeting with business connections. As millions of Americans and global citizens work from home during the pandemic, the cyber criminals and pranksters are at home working on their craft as well.

Below are some of the risks associated with using Zoom and a list of Quick Tips that can be used to reduce the risks. The Risks and Concerns are noted, followed by a Boot The Party-Crasher tip to kick out any troll that drops in unexpectedly. Additional lists of tips are provided based on the different types of meetings that you may be hosting with Trusted Participants or External Participants.

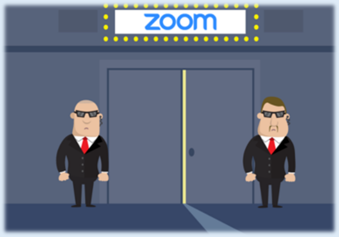
When using Zoom, or any teleconference platform, consider the following options before scheduling an online meeting.

Quick Tips

1. Never use your personal meeting ID
2. Always use a meeting password and share it securely
3. Use Zoom's waiting room feature to approve guests
4. Mute audio and disable video for meeting participants
5. Do not share your meeting link on social media or other public websites
6. Turn off screensharing for everyone except the meeting host/co-host
7. Lock the meeting after the meeting starts
8. Always accept and install the Zoom application updates as soon as available

Risks and Concerns

- A participant shares 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)
- A participant 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
- A participant shares your meeting invite publicly
- A party-crasher joins 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



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

Trusted Participants

You may setup a meeting with a small trusted group of colleagues or friends. In this scenario, you know everyone joining the meeting, they are trusted colleagues from within your organization. You want to share video and do not expect any party-crashers because you shared the link and meeting password privately.

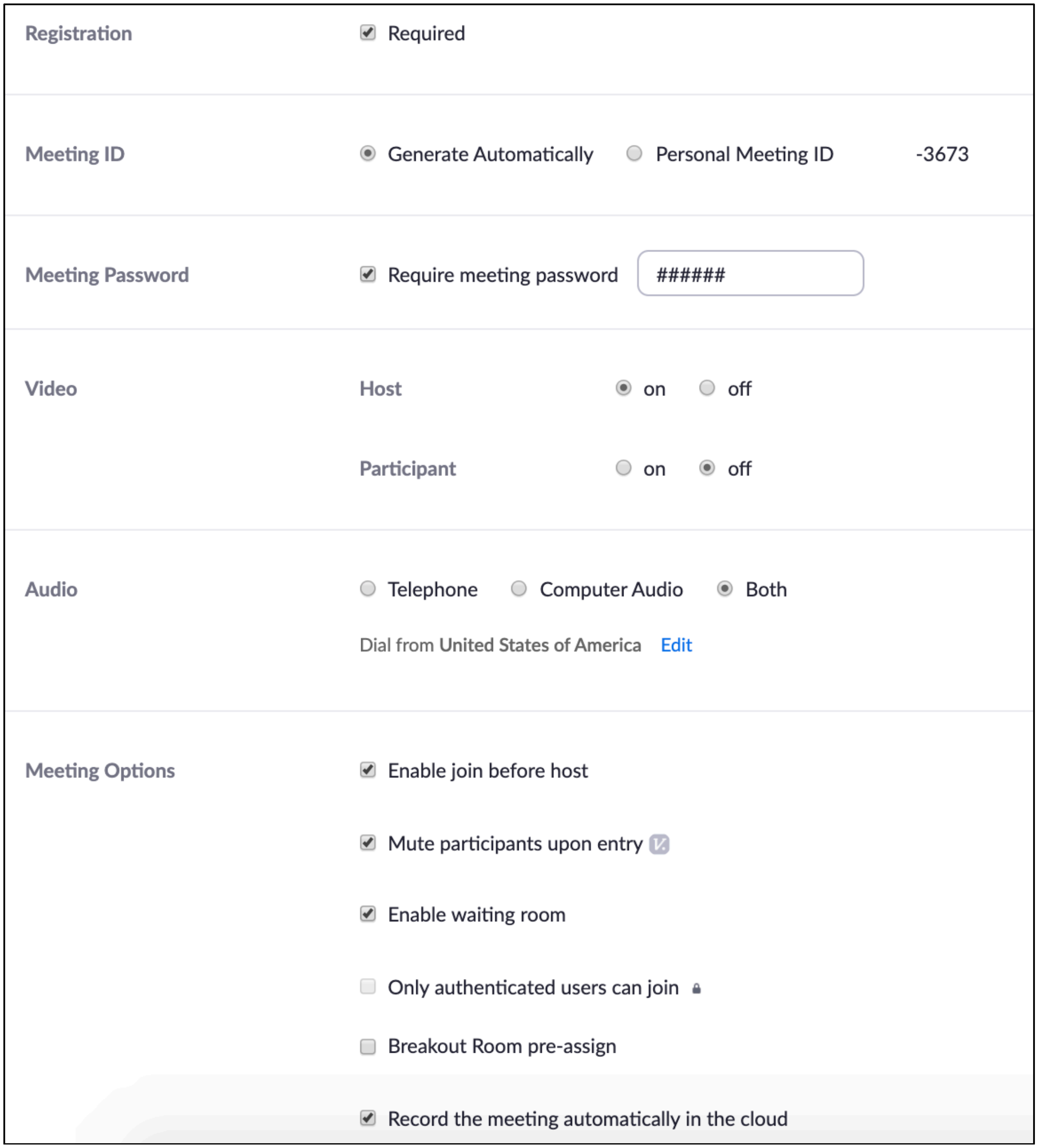
1. Never use your personal meeting ID
2. Do not share your meeting link on social media or other public websites
3. Always use a meeting password and share it securely
4. Mute audio for all participants upon entry to the meeting
5. Turn off screensharing for everyone except the meeting host/co-host and give control to other participants only when necessary
6. Lock the meeting after expected participants have joined

External Participants

You want to have a meeting with colleague from another organization or the community. We shouldn’t assume these participants have the best intentions. In this scenario, you have invited people to join the meeting that may share your link with other people due to the nature of the meeting. You want to share your screen and it is not important for participants to share their video or personal information. This is a full lock-down scenario where the host has control and guests are viewing/listening but not participating in the presentation or discussion.

1. Never use your personal meeting ID
2. Do not share your meeting link on social media or other public websites
3. Use Zoom's waiting room feature to approve guests
4. Add a personal message to the waiting room
5. Mute audio and disable video for meeting participants
6. Do not select *Enable join before host*
7. Turn off screensharing for everyone except the meeting host/co-host
8. Disable private chat sessions
9. Lock the meeting after the meeting starts to prevent late party-crashers
10. Turn off file transfer
11. Turn off annotations
12. Record the meeting in the cloud

Meeting Options in Zoom



Registration	☑ Required
Meeting ID	● Generate Automatically ○ Personal Meeting ID -3673
Meeting Password	☑ Require meeting password ######
Video	Host ● on ○ off Participant ○ on ● off
Audio	○ Telephone ○ Computer Audio ● Both Dial from United States of America Edit
Meeting Options	☑ Enable join before host ☑ Mute participants upon entry ☑ Enable waiting room □ Only authenticated users can join □ Breakout Room pre-assign ☑ Record the meeting automatically in the cloud

Additional Tips

- You can still edit the meeting after it is setup, before the meeting begins
- You can add an alternate host from within your organization in case you cannot login right on time or want someone to monitor the waiting room
- Learn about the features before formal meetings or before meetings with public participants
- Visit the Zoom Help Center to search for topics

Zoom Meeting Setup

Registration Required (Zoom instructions)

- Unchecked – participants are not asked for any information and anyone with the link can join
- Checked – requires participant to provide selected information in order to access the meeting
  - Automatically approve
  - Manually approve

Meeting ID

- Automatically generates a meeting ID that participants use when calling in
- Personal Meeting ID is auto-generated by Zoom (NOT RECOMMENDED)

Meeting Password

- Require meeting password
  - Unchecked – any guest with the link can join your meeting
  - Checked
    - Automatically generates a 6-digit meeting ID to share with participants
    - Create your own meeting ID to share with participants

Video

- Host
  - On – video is on when meeting starts
  - Off – video is off when meeting starts
- Participant
  - On – video is on when meeting starts
  - Off – video is off when meeting starts

Audio

- Telephone – participants can connect by phone using dial-in numbers to enter the meeting
- Computer Audio – participants can use only computer audio, cannot dial-in
- Both – participants can connect using dial-in numbers and computer audio
  - Some computers do not have a microphone or speakers
  - Sometimes the participant is in a public space and use the phone for privacy while using the computer to view any screensharing or chat

Meeting Options

- Enable join before host
  - Unchecked – participants cannot join the meeting until the host has started the meeting
  - Checked
    - Allows participants to join the meeting before the host has started the meeting
    - Depending on other settings, participants may talk, share video, screenshare, file share, and chat while the host is not present
- Mute participants upon entry

  - Unchecked – allows participants to freely talk and play audio
  - Checked – disables participant audio upon entry into the meeting
- Enable waiting room
  - Unchecked – allows participants to enter the meeting immediately after clicking the meeting link or dialing in
  - Checked – places participant into a virtual waiting room until the host accepts the participant into the meeting
- Only authenticated users can join
  - Unchecked – allows participants to enter the meeting without providing a username and password
  - Checked – participant are required to successfully provide a username and password in order to enter the meeting
- Breakout Room pre-assign
  - Unchecked – participants are not assigned to a breakout room
  - Checked – participants are assigned to a breakout room before the meeting begins
- Record the meeting in the cloud
  - Unchecked – recording will not begin when the meeting starts, but the host can still record using the Record option anytime during the meeting
  - Checked – recording will begin immediately when the meeting starts

Zoom-bombers, trolls, and party-crashers

According to a CNN interview with Zoom's CEO, Eric Yuan, they are now focused on security and privacy. Prior to this, Zoom was definitely gaining traction in the teleconference realm with capabilities to quick link meeting attendees with a URL or phone number to dial-in to an online meeting. The easy-to-use features in Zoom include live video from all participants, audio with option to mute, call-in from phone linked to online participant, screen-sharing for all participants, text chat for all participants, closed-captioning, and recording sessions to the cloud. With a variety of other options, Zoom quickly became a very popular work-from-home app due to the COVID-19 pandemic and government restrictions to go out only for work and essential services, known as stay-at-home orders. An April 1st blog said that the number of daily meeting participants in March was 200 million, up from 10 million in December 2019.

Zoom has announced that it would focus on privacy and security issues for the next 90 days and skip feature updates. Despite the company's promises to improve security and the FBI's steps to mitigate teleconference hijacking, some school districts have decided to ban Zoom and use Microsoft Teams instead. To make the Zoom platform user-friendly, no account or software is needed in order to access a Zoom meeting link from anywhere in the world. This has provided Zoom-bombers, trolls, and party-crashers with the ability to unleash mayhem on meetings by showing pornographic materials, screaming obscenities, and disrupting meetings by finding Zoom links on social media or guessing meeting id's.

As millions of Americans and global citizens work-from-home during the pandemic, the cyber criminals and pranksters are staying at home to work on their craft as well. With the impact of the Zoom vulnerabilities reaching many age ranges from elementary school to professionals with decades of work experience, it brings cybersecurity and privacy to the forefront for everyone. Hopefully this momentum to raise public awareness about these topics does not get swept away in the midst of the pandemic.

In case you use Zoom, or any teleconference platform, consider the following options before scheduling your online meeting.

1. Never use your personal meeting ID
2. Always use a meeting password and share it securely
3. Use Zoom's waiting room feature to approve guests
4. Mute audio and disable video for meeting participants
5. Do not share your meeting link on social media or other public websites
6. Turn off screensharing for everyone except the meeting host/co-host
7. Lock the meeting after the meeting starts
8. Always accept and install the Zoom application updates as soon as available

Professor Tobi West, CISSP, GCFE
CIS/CST/CYBR Department Chair
Coastline College
Cyber Center

References

If you would like to read more on these topics, below is a variety of articles used to develop this document.

BBC. (7 Apr 20). Zoom banned by Taiwan's government over China security fears. BBC News Services. Retrieved from https://www.bbc.com/news/technology-52200507

Dai, S. (7 Apr 20). Zoom’s security backlash points to bigger threats in coronavirus-led telecommuting wave, experts say. South China Morning Post. Retrieved from https://www.scmp.com/tech/enterprises/article/3078566/zooms-security-backlash-points-bigger-threats-coronavirus-led

Hodge, R. (8 Apr 2020). Zoom: Every security issue uncovered in the video chat app. C|NET. Retrieved from https://www.cnet.com/news/zoom-every-security-issue-uncovered-in-the-video-chat-app/

Kamenetz, A. (6 Apr 20). Schools Ditch Zoom Amid Concerns Over Online Learning Security. National Public Radio. Retrieved from https://www.npr.org/sections/coronavirus-live-updates/2020/04/06/828087551/schools-ditch-zoom-amid-concerns-over-online-learning-security

Keane, S. (6 Apr 20). School districts reportedly ban Zoom over security issues. C|NET. Retrieved from https://www.cnet.com/news/school-districts-reportedly-ban-zoom-over-security-issues/

Krebs. (2 Apr 20). ‘War Dialing’ Tool Exposes Zoom’s Password Problems - CSO | The Resource for Data Security Executives. Krebs on Security. Retrieved from https://www2.cso.com.au/vendor_blog/6/krebs-on-security/24072/war-dialing-tool-exposes-zooms-password-problems/

Lakshmanan, R. (2 Apr 20). Zoom Caught in Cybersecurity Debate — Here's Everything You Need To Know. Retrieved from https://thehackernews.com/2020/04/zoom-cybersecurity-hacking.html

Langley, H. (8 Apr 20). Google has banned the Zoom app from all employee computers over 'security vulnerabilities'. Business Insider. Retrieved from https://www.businessinsider.com/google-bans-zoom-from-employee-computers-due-to-security-concerns-2020-4

Lyons, K. (5 Apr 20). Zoom CEO responds to security and privacy concerns: ‘We had some missteps’. Retrieved from https://www.theverge.com/2020/4/5/21208636/zoom-ceo-yuan-security-privacy-concerns

Setera, K. (30 Mar 20). FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic. Federal Bureau of Investigations (FBI). Retrieved from https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

Vigliarolo, B. (3 Apr 20). How to prevent Zoom bombing: 5 simple tips. TechRepublic. Retrieved from https://www.techrepublic.com/article/how-to-prevent-zoom-bombing-5-simple-tips/

Wardle, P. (30 Mar 20). The 'S' in Zoom, Stands for Security. Retrieved from https://objective-see.com/blog/blog_0x56.html

Zoom Blog. (20 Mar 20). How to Keep Uninvited Guests Out of Your Zoom Event. Retrieved from https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/