Conducting Zoom Calls with Confidence

A visual guide to adjusting your global settings and best practices for safe online meetings

Rafael Brinner, Director of Jewish Community Security

April 28, 2020
Overview

This visual guide is designed to help you navigate the virtual landscape of Zoom meetings as safely as possible. It covers:

- How to upgrade your Zoom software to the latest version.
- Five best practices for making your Zoom calls:
  - harder to intentionally disrupt
  - easier to manage if crashers show up
- How to report an incident
Upgrade to the latest version of Zoom (for Windows)
Upgrade to the latest version of Zoom (for Mac OS)
Five Best Practices

1. Adjust your account settings
2. Use the Registration feature
3. Appoint a bouncer
4. Lock the room
5. Record your call

Block unwanted visuals
Restrict written communication
Adjust your account settings

**Meeting**
- Schedule Meeting
- In Meeting (Basic)
- In Meeting (Advanced)
- Email Notification
- Other

**Recording**
- Schedule Meeting

**Telephone**
- Host video
  - Start meetings with host video on
- Participants video
  - Start meetings with participant video on. Participants can change this during the meeting.
- Audio Type
  - Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that all participants follow the instructions you provide for using non-Zoom audio.
  - Telephone and Computer Audio
  - Telephone
  - Computer Audio
Avoid using the same meeting link recurrently or using short or guessable passwords.

<table>
<thead>
<tr>
<th>Meeting</th>
<th>Recording</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Meeting</td>
<td>Join before host</td>
<td>Use Personal Meeting ID (PMI) when scheduling a meeting</td>
</tr>
<tr>
<td>In Meeting (Basic)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In Meeting (Advanced)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Notification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Join before host**
Allow participants to join the meeting before the host arrives

**Use Personal Meeting ID (PMI) when scheduling a meeting**
You can visit Personal Meeting Room to change your Personal Meeting settings.

**Use Personal Meeting ID (PMI) when starting an instant meeting**

**Only authenticated users can join meetings**
The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.

**Require a password when scheduling new meetings**
A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.
Disabling embedded passwords adds inconvenience but can also deter crashers looking for the easiest meetings to disrupt.
If you are not relying on the chat function, disable it to prevent crashers abusing it.
Adjusting these controls keeps crashers from sharing offensive visual content or drawing on the slides.
Note you can also change sharing permissions during the meeting.
## Meeting

<table>
<thead>
<tr>
<th>Schedule Meeting</th>
<th>Recording</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Meeting (Basic)</td>
<td>In Meeting (Basic)</td>
<td>Allow participants to rename themselves</td>
</tr>
<tr>
<td>In Meeting (Advanced)</td>
<td>Email Notification</td>
<td>Hide participant profile pictures in a meeting</td>
</tr>
<tr>
<td>Email Notification</td>
<td>Other</td>
<td>All participant profile pictures will be hidden and only the names of participants will be displayed on the video screen. Participants will not be able to update their profile pictures in the meeting.</td>
</tr>
</tbody>
</table>

### In Meeting (Advanced)

<table>
<thead>
<tr>
<th>Virtual background</th>
<th>Consider Enabling</th>
<th>Waiting room</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.</td>
<td>Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled.</td>
<td></td>
</tr>
</tbody>
</table>
Use the Registration feature

Registration adds a step, but it lets you know ahead who will be on your call.
Use the Registration feature

Select Manually Approve if the number of people you anticipate does not make this burdensome.
Use the Registration feature

Require fields like Zip Code and Organization so that anomalies stand out and supply data points for verifying people you don’t recognize.

NOTE: You can select the Questions & Comments field to solicit input ahead of your meeting.
Use the Registration feature

Click **View** to check who has registered and identify those who are unfamiliar.

- **My Meetings** > Manage "Conducting Zoom Calls with Confidence"

<table>
<thead>
<tr>
<th>Registration</th>
<th>Email Settings</th>
<th>Branding</th>
<th>Poll</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Attendees</td>
<td>Registrants: 55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration Options</td>
<td>Automatically Approved</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- ✗ Send an email to host
- ✔ Close registration after meeting date
3 Appoint a bouncer

Identify co-hosts and assign them distinct tasks, such as muting open mics or removing disruptive people.
Lock the room

Use the Lock feature if everyone you need has arrived in the meeting, or if you can afford to exclude late-comers.

NOTE: If someone drops due to connection problems, they won’t be able to rejoin.
Record your call

Even if you don’t record the whole meeting, you or a co-host should hit record if a crasher engages in unwelcome behavior.

Video footage, and any relevant chat transcript, serves as evidence against crashers.
Five Best Practices

1. Adjust your account settings
2. Use the Registration feature
3. Appoint a bouncer
4. Lock the room
5. Record your call

Block unwanted visuals
Restrict written communication
How to report an incident

If someone explicitly threatened you or your organization with violence, call 911.

Report Internet crime of any sort, including unauthorized access to a Zoom meeting, by filing a complaint with FBI’s Internet Crime Complaint Center: www.ic3.gov

Report hate speech or a hate incident to the Anti-Defamation League: https://www.adl.org/reportincident