Oregon Department of Justice's
CIVIL RIGHTS UNIT

Frequently Asked Questions and Additional Resources to Prevent or Respond to Zoom Bombing

What is zoom bombing?

Zoom bombing is unwanted, disruptive conduct during a virtual meeting intending to derail the meeting and harass and offend attendees. It is an intrusive act and a form of cyber-harassment. Examples of zoom bombing include interrupting a set meeting agenda by showing inappropriate or hate images, spewing profanity or bigoted slur words, trolling, threatening attendees, filling chat fields with gibberish or slurs to prevent communication amongst attendees, or repeatedly making offensive comments. Perpetrators often hide behind fake names, leave their cameras off, use voice moderators, and even use a VPN to hide their IP address so they cannot be detected.

Why are we only talking about Zoom? Can't this happen on any platform?

Zoom bombing is a general, colloquial term used to describe when a video conference is being disrupted, but it can happen on any platform, not just Zoom. The term originated during the Covid-19 pandemic when people and organizations widely used video conference applications and online platforms for government business, work, church, private business, and school.

Is zoom bombing a crime in Oregon?

Zoom bombing may constitute a crime in Oregon if explicit, specific, and imminent threats are made. Otherwise, zoom bombing is commonly not a crime, but rather is classified as a non-criminal bias incident under Oregon law.

What are the effects of zoom bombing?

Some of the effects of zoom bombing are abrupt endings of public meetings and schools suspending their online classes. Additionally, as there is often a bigoted component to perpetrators' conduct, zoom bombing has damaging and harmful effects to communities impacted by inequity and people belonging to a protected class.

I’m hosting an online meeting. What registration, regulations, and additional safety considerations should I prepare?

U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) created guidance on how to secure video conferencing. Some general and some Zoom-specific instruction is below. In addition to this guidance, individuals and organizations should assess risks of systems and software they are using and implement security measures.

1. **Secure connection** – default settings for Wi-Fi networks and many video conferencing tools are not secure. Here are some tips for connecting securely:
    a. Change passwords to strong and complex passwords for your router and Wi-Fi network.
    b. Consider choosing a different name for your Wi-Fi network if you do not want others to recognize your network.
    c. Make sure your router is configured to use Wi-Fi Protected Access 3 (WPA3) or Wi-Fi Protected Access 2 (WPA2). Check CISA’s tips on Home Network Security for more information.

2. **Control Access** – enable features that allow you to control who can access your video conference and calls. Here are some tips for controlling access to your online meetings:
    a. Require a password or code to attend the event – having this feature will allow only those with the passcode to access the scheduled meeting. Here is an article from Zoom on how to add passcodes to your meetings. Passwords can be set at the individual meeting level or can be enabled at the user, group, or account level for all meetings and webinars.
    b. Enable “waiting room” feature – this will allow the host to admit participants individually and will prevent participants from joining the meeting before the host. To change this setting in Zoom, sign-in to web portal and click “Settings” from the main menu. Under the “Meeting” section, find the “Security” and turn on the “Waiting Room” toggle.
    c. Lock the event – once all participants have joined or when the meeting has started, you have the option to lock the meeting to prevent other participants from joining, even if they have the meeting ID and password. To lock the meeting in Zoom, click on the “Security” toolbar. From the menu, click on “Lock Meeting.” The message “You

have locked the meeting. No one else can join" will then appear on the screen.

d. Ensure that you are able to admit and remove attendees manually to expel any disruptive participants. To remove a participant in Zoom, click the "Security" toolbar then click "Remove Participant." A "Remove Participant" window will appear on the right. Click on "Remove" next to the participant you want to remove.

3. **Manage file, screen sharing and recordings** – Consider disabling or limiting file and screen sharing to ensure only trusted individuals are able to share.

   a. Disabling file transfer will help keep the participants from sharing or receiving unsolicited pictures, malicious links, and files. Here is more information on managing file transfers in Zoom team chat.

   b. Disabling screen sharing prevents unwanted interruptions and stops participants from showing inappropriate screens and images. This feature can easily be turned on and off from Zoom's security menu, as well as from the screen sharing menu.

   c. Inform participants that the event is being recorded. To record a meeting in Zoom, simply hit the "Record" button on the toolbar.

4. **Update software regularly** – ensure all applications and devices are updated to the latest versions to protect from intruders, hackers, ransomware, malware, and data breaches. Enable automatic updates for your software. Check CISA's Understanding Patches and Software Updates for more information.

5. **Require participants to register** – as an added layer of security, consider requiring participants to register by providing their name and email. To enable registration for a meeting, sign in to Zoom web portal and click "Meetings" from the main menu. Click "Schedule a Meeting" or edit an existing meeting. In the "Registration" section, select the "Required" checkbox and click "Save." Here is more information on how to schedule and customize a Zoom meeting with registration.

6. **Do NOT use Personal Meeting ID (PMI)** – a Personal Meeting ID is a 9 to 11-digit number that is assigned to your account and allows you to access your Personal Meeting Room. Anyone with access to your PMI can enter your meeting room without an invitation. To disable the use of PMI, sign in to the Zoom web portal and click "Settings" from the main menu. Under the

"Meeting" section, find the "Schedule Meeting" and turn off the "Enable Personal Meeting ID" toggle.

7. **Muting** – to avoid disruptions, all participants should be muted when they join the meeting. To enable this feature, sign in to the Zoom web portal and click "Settings" from the main menu. Under the "Meeting" section, find the "Schedule a Meeting" and turn on the "Mute all participants when they join a meeting" toggle.

8. **Turn off Annotation** – turning off annotation will prevent participants from writing all over a screen share/whiteboard. To disable participant annotation, sign in to the Zoom web portal and click "Settings" from the main menu. Under the "Meeting" section, find the "In Meeting (Basic)" and turn off the "Annotation" toggle.

9. **Disable *mask phone number* in the participant list** – when this setting is enabled, the phone numbers of users dialing into a meeting will be masked in the participant list. To disable this setting, sign in to the Zoom web portal and click "Settings" from the main menu. Under the "Audio Conferencing" section, turn off "Mask phone number in the participant list" toggle.

10. **Disable Private Chat** – disabling private chat will prevent participants from chatting in the meeting or sending inappropriate messages to other participants. To disable chat, click on the "Security" toolbar. From the menu, make sure that the "Chat" is not checked. You can also manage the chat feature by clicking the "Chat" toolbar. Click the ellipsis located at the bottom of the Chat window and select "No One" under the "Participants Can Chat With."

11. **Disable start video** – disabling videos will prevent participants from streaming anything (including inappropriate materials) without the host's permission. To disable participants from starting videos, click on the "Security" toolbar. From the menu on "Allow All Participants to", uncheck "Start Video."

12. **Disable participants from renaming themselves** – participants are automatically given names based on their Zoom account or their computer's username. To prevent them from renaming themselves including using a slur as a name, click on the "Security" toolbar. From the menu on "Allow All

Participants to," uncheck "Rename Themselves." Another option is to click the "Participants" toolbar. On the "Participants" box, click the ellipsis on the bottom. Uncheck "Allow Participants to Rename Themselves."

13. **Turn on Co-Host feature** – having one or two co-hosts depending on the size of the meeting can be helpful in managing a Zoom meeting. The host acts as the traditional meeting chair while the co-host manages the participants and meeting controls such as muting, hand raising, and intrusions. To assign a co-host, hover over the future co-host's name, click "More," and then select "Co-Host."

What tips do you have for responding to zoom bombing?

It is important to document and preserve any evidence and to provide immediate support to those who may have been affected.

1. **Preserve as much information as possible**. Record the incident. If your meeting is not being recorded, hit the "Record" toolbar immediately to capture the incident. Take as many screen shots as possible using your computer or other device such as your cell phone. To save chat messages, click the "Chat" toolbar. At the bottom of the Chat window, click the ellipsis then click "Save Chat." Here is more information on how to store and view chat history.

2. **Take immediate action to stop the conduct**.
   a. If a zoom bomber is sharing their screen, immediately un-share their screen by clicking the "Security" toolbar. Under "Allow All Participants to:" uncheck the "Share Screen."
   b. To mute, click the "Participants" toolbar. At the bottom of the Participants box, click "Mute All". A window will appear on the screen that says, "Mute all current and new participants" and an option to "Allow Participants to Unmute Themselves." Click "No."
   c. Remove disruptive participants by clicking the "Security" toolbar then click "Remove Participant." A "Remove Participant" window will appear on the right. Click on "Remove" next to the participant you want to remove.

3. **Prepare in advance**.
   a. Consider creating a policy and procedure or a code word if zoom bombing occurs.

b. Assign someone who will be responsible in preserving any information.
c. Assign someone to interrupt the speech with their voice in real time and make a statement.

4. **Make a statement** – The person from your organization assigned to make a statement should acknowledge the incident, condemn the speech/conduct, assert a commitment to safety and an anti-hate space, and recognize the impact of hate speech and bias to people who were directly targeted by the attack.

5. **Safety and care –** End the meeting if necessary and encourage everyone to take care of themselves. Provide resources for support. Offer to meet after the meeting to debrief. Consider hosting a community conversation in the following days to hear from those impacted. Share safety steps and policy planning to the extent possible.

The Anti-Defamation League (ADL) has published additional Steps To Take During a Zoombombing Incident.

I work for local government. Are there different rules for us? Can I interrupt people during their public comment if it's hate speech?

Oregon DOJ is prohibited from giving you legal advice on this matter. However, there are several resources that specifically address these questions, including:

- Attorney General's Public Records and Meetings Manual (2019)
- League of Oregon Cities Legal Guide to Handling Disruptive People in Public Meetings (2023)
- Oregon Department of Administrative Services Virtual Public Meetings Guide for State Agencies (2024)
- Oregon Government Ethics Commission for enforcement, complaints or requesting advice regarding public meetings law
- ADL's Toolkit for Responding to Extremist Disruptions at Public Meetings

Where should I report zoom bombing?

- Report the incident to FBI's Internet Crime Complaint Center or IC3.
- If specific, explicit, or imminent threats were made, or if your local law enforcement agency takes reports of bias incidents, report to your local law enforcement agency.

- Report to the Bias Response Hotline for data purposes. Participants who were targeted can report to the Bias Response Hotline to receive support and services.
- Reporting inappropriate behavior on Zoom.

I've been asked to conduct a presentation at a virtual meeting. Do you have any suggested questions I should ask the host to be sure the meeting will be a safe space?

- Have you previously had zoom bombing occurrences?
- Do you plan to share about the event on traditional or social media?
- Are you requiring participants to register?
- Will the event be recorded?
- Do you have your security settings set to default or do you have certain features disabled (chat, video, screen sharing, name change, waiting room, etc.)?
- What platform will this be hosted on?
- Do you have the most up to date version of the software?
- Do you have a co-host assigned to virtual security?
- Do you have a plan in case zoom bombing happens?

Do you have resources if I'm using other platforms/video conferencing applications on how to connect securely and manage virtual meetings?

- Microsoft Teams
- Cisco WebEx
- Adobe Connect
- GoTo Webinar
- GoTo Meeting
- Other secure applications for private video chats

Additional Sources

https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf
https://diversity.tufts.edu/resources/how-to-respond-to-a-zoombombing-in-real-time/
Privacy and Security for Zoom Video Communications