Zoom-bombing prevention guide

for Young Green member organisations

Compiled by: Michael J. Oghia, Meri Baghdasaryan, and Weronika Koralewska of the Digital-X Working Group (Cooperation and Development Network Eastern Europe)

Contact emails:

mike.oghia@gmail.com (Digital-x WG member)

ledina@cdnee.org (Digital-x WG coordinator)

communications@fyeg.org (FYEG Communication Officer)

Overview: This short guide is meant to help anyone working in sensitive fields (such as political groups, journalists, or activists) or with marginalised groups better prepare/safeguard themselves and their online activities while using video conferencing software, especially the Zoom platform.

Background: With the new normal caused by the COVID-19 pandemic, we have to find new ways to foster solidarity, build community, and stay connected to one another. As a result, we are increasingly relying on digital tools, specifically video conferencing software such as Skype and Zoom. A phenomenon that has arisen recently is known as "Zoom-bombing." This refers to unwanted intrusion into a video call by a troll or bad actor that can range from disruptive to downright traumatising. Especially given that our organisations are already prone to harassment, it is imperative that, regardless of the platform chosen, we do not give bad actors opportunities to invade our spaces by taking measures to safeguard our privacy, security, and mental well-being. This guide is meant to provide some quick pointers about what anyone seeking to host an online meeting, specifically on Zoom, can do to protect the integrity of the meeting/webinar/call, and prevent bad actors from hijacking a call to display disruptive or disturbing content.

The Problem: The way that applications like Zoom and Jitsi are built means that they are relatively easy for anyone to use. This is, in part, due to the way its meeting ID system works. Anyone with the meeting ID can join a call. According to the Electronic Frontier Foundation (EFF), however, bad actors can find your meeting in one of two ways: (1) they can cycle through random meeting IDs until they find an active one, or (2) they can take advantage of meeting links and invites that have been posted in public places, like Facebook groups, Twitter, or personal websites. Thus, protecting yourself boils down to controlling who can enter your meeting and keeping your meeting IDs private.

Solutions to/preventative measures for Zoom-bombing:

1. **Passwords** – Most importantly: **use a password**, and do not widely share that password. Inspect the meeting invite links carefully. Be aware that if you share the meeting link publicly, such as on Facebook or Twitter, its password will also become public. Make sure the "require a password when scheduling new meetings" feature is enabled. Regarding the Zoom client, it is also recommended to use a password manager (preferably across an

organisation) to better manage/store sensitive credentials.

2. **Registration** – Second most important: **require registration for every call/meeting**. While this will likely limit spontaneous joining by trusted friends/members, it will provide a key layer of security and privacy.

- **Public meetings and anonymity –** If you need to have a public meeting or want to preserve the anonymity of your participants, you can also use the following step. The host should enter the Zoom meeting and before 'starting' it, share their screen and click the "More" button, then select disable "attendee annotation." At the bottom of the Participants list, they should press Mute All and deselect "Allow participants to unmute themselves." The host can then selectively unmute attendees as needed.

Additional measures:

- **Security settings** – Familiarize yourself with security settings before setting up a meeting, and understand which tools are available during a meeting (Zoom details how on their blog).
- **Updated software** – Make sure your Zoom client (or any software for that matter) has the latest updates, which include security updates as well as user interface updates that offer greater controls to the meeting host.
- **Set up your own two-factor authentication** – No need to share the meeting link and password publicly. Instead, you can generate the meeting link and share it publicly, but send the password through private messaging.
- **Avoid "Join Before Host" –** Instead, enable the "waiting room" feature, which will allow you to monitor and approve who joins the meeting and prevent meeting hijacking.
- **Disable "file sharing" –** This may help to prevent the sharing of graphic material, especially in the form of animated gifs in the chat box.
- **Lock the meeting** – After all meeting participants are approved to join in, lock the meeting.
- **Screen sharing –** Lockdown screen-sharing by only allowing hosts to share a screen.
- **Manage meeting chat –** Monitor the meeting chat and adjust its settings (e.g., disable private chats). This will also help to prevent sharing of animated GIFs and other files in the chat.
- **Remove unwanted or disruptive participants** – Per the advice from Zoom, you can mouse over a participant's name in the Participants menu, and several options will appear, including Remove. Click that to kick someone out of the meeting.
- **Disable participants' video** – In case there are unwanted, distracting, or inappropriate gestures on video, you may disable the video for some or all participants.
- **Virtual backgrounds –** For increased privacy, you can use a virtual background.

You can also see an infographic with a more visual representation of this information here.

Remember: Security is incredibly important to the work we do and the people in our community. It is also our responsibility to keep our communities safe, especially since we are often targeted for the people we stand up for and causes we fight for.

What to do if it happens and how to deal with trauma?

- If something happens during a call, first of all reach out to Zoom via Twitter (@zoom_us) or through their website, and they will conduct a formal investigation. It is important that you elevate such cases to them so they can ban/block bad actors and potentially trace their IP address in order to report them to law enforcement officials.
- If you see disturbing content, there (unfortunately) does not seem to be any kind of resource that is there to help (such as a hotline or some kind of chat resource).
- Resources meant to help journalists deal with traumatic imagery/moments, such as this one and this one, may provide good tips, as well as the OnlineSOS Action Plan for Emotional Well-Being and PEN America's Online Harassment Field Manual, which includes advice from a psychologist on how to manage/recover from harassment and other online abuse.
- It is important to remember, though, that if you feel traumatized, please talk to someone you trust and potentially seek advice from a mental health professional.
- Whatever you do, know that if you feel trauma, it is perfectly OK to feel bad, and it's OK to ask for help and seek help.

Important reminder about recording a meeting – If the call/meeting is being recorded and disturbing or especially illegal content is displayed, know that you may be liable for that if it's uploaded online or stored on your device. Although this may seem self-evident, it is important to remember that many meetings are recorded straight to the cloud or directly to a computer, so it is our responsibility to make sure we do not unwittingly spread such content.

RESOURCES

Zoom alternatives/other digital tools:

- Jit.si – https://meet.jit.si/. Other related options to help ease pressure on Jit.si"s servers include: https://www.infomaniak.com/en/meet, https://calls.disroot.org/, https://www.fairkom.eu/en/fairmeeting, https://meet.freepressunlimited.org, and https://meet.collective.tools/
- Tox – https://tox.chat/
- Signal – https://www.signal.org/
- Other video chatting services: Skype, GoToMeeting, and WebEx. For more information, see this guide from DiploFoundation.

Resources to review with even more tips and guides for how to enable security features in Zoom:

- Beware of ‘Zoom-Bombing’: Screen Sharing Filth to Video Calls (TechCrunch)
- FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic (FBI)
- Harden Your Zoom Settings to Protect Your Privacy and Avoid Trolls (EFF)

- How to Keep Uninvited Guests Out of Your Zoom Event (Zoom)
- How to Prevent Zoom-Bombing (PC Mag)
- Privacy & Security for Zoom Video Communications (Zoom)
- Settings for Preventing Zoom-Bombing (UC Berkeley)
- Tips to Make Your Zoom Gatherings More Private (Mozilla)
- What You Should Know About Online Tools During the COVID-19 Crisis (EFF)
- Zoom-bombing Self-defense: A Technical Guide (Palante Tech Coop)

Additional security and online safety resources:

- Committee to Protect Journalists (CPJ) – Journalists' Safety Guide and Safety Kit, which includes cybersecurity resources as well. CPJ also created a Digital Safety Kit in English, Español, Français, and Русский
- Electronic Frontier Foundation (EFF) – Surveillance Self-defense (SSD): Tips, tools, and how-to's for safer online communications
- Frontline Defenders – Security-in-a-box: Digital security tools and tactics
- Global Forum for Media Development (GFMD) – Journalists' Safety Resource Centre
- Global Investigative Journalism Network (GIJN) – Digital security
- Reporters Without Borders (RSF) – Digital Security for Journalists, a help desk featuring information on training, digital security guides, and FAQs/dangerous misconceptions
- Tactical Technology Collective (Tactical Tech) – Digital security & privacy
- Totem (Free Press Unlimited and Greenhost) – offers free online courses in English, French, and Farsi that cover a wide array of digital security-related topics
- WAN-IFRA – Top cybersecurity tips and tools for journalists
- We Live Security – Cybersecurity for journalists and the news media

This document is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0).