Z

Zoombombing: Prevention and Meeting Incident Response

Zoombombing is unauthorized disruption of an online meeting. Learn how links leak, which host controls prevent abuse, and how to respond quickly.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What is Zoombombing?
02 How unwanted participants get in
03 Secure a meeting before it starts
04 What to do during Zoombombing
05 After the incident
06 Zoombombing vs. account compromise

Quick answer: Zoombombing is unauthorized entry into a Zoom or other online meeting to disrupt, harass, display offensive content, record participants, or gather information. Use a unique meeting ID, a passcode or waiting room, restricted screen sharing, and

controlled invitations. During an incident, suspend participant activity, remove and report the intruder, lock the meeting, preserve evidence, and replace exposed meeting details.

01 What is Zoombombing?

Zoombombing is a popular name for meeting bombing: an uninvited person or bot joins an online session and abuses participant features. The term began with Zoom, but the same pattern can affect any conferencing platform. Disruption can include shouting, screen sharing, offensive chat, impersonation, unwanted recording, link posting, or attempts to trick participants.

An incident does not necessarily mean the platform was hacked. Frequently, a valid meeting link, ID, passcode, or calendar invitation was posted publicly, forwarded, reused, guessed, or taken from a compromised account. Weak meeting settings then give the entrant too much capability.

02 How unwanted participants get in

- A join link is posted on a public website, social network, or open group.
- The same Personal Meeting ID or recurring link is reused for unrelated audiences.
- A calendar or email account is compromised, exposing invitations.
- Anyone with the link can join before the host or bypass meaningful admission checks.
- Participants forward an invitation, intentionally or accidentally.
- A public event uses ordinary meeting controls when a webinar-style format would be safer.

03 Secure a meeting before it starts

1. **Use unique meeting details:** schedule a new ID for sensitive or publicized sessions instead of reusing a Personal Meeting ID.
2. **Require admission control:** enable a passcode, waiting room, registration, or authenticated-user requirement appropriate to the audience.

3. **Share invitations privately:** do not publish a one-click link containing the embedded passcode. Send it only to intended participants.
4. **Limit participant powers:** make screen sharing host-only by default and review chat, file transfer, annotation, rename, unmute, and remote-control settings.
5. **Assign moderation:** add a co-host for larger events, start early, and confirm the Security controls before admitting people.
6. **Choose the right format:** use a webinar or broadcast mode when the audience does not need full participant privileges.

A passcode embedded in a public join link does not remain secret. A waiting room also needs active moderation: compare names with registration information and challenge unexpected entrants when appropriate.

04 What to do during Zoombombing

Use the host's Security controls to suspend participant activities or immediately disable screen sharing, chat, annotation, and unmuting. Remove the disruptive participant, report them through the platform when available, and lock the meeting after legitimate attendees are present. Do not argue with the intruder or open links they post.

If disruption continues, end the meeting for everyone and create a new session with new credentials. Send the replacement invitation through a trusted private channel. For a serious threat, targeted harassment, exposure of sensitive information, or illegal content, follow organizational safety and law-enforcement procedures.

05 After the incident

- Preserve the meeting ID, time, participant list, chat, screenshots, moderation actions, and relevant audit logs.
- Remove public posts containing the invitation and replace the meeting ID and passcode.

- Review whether a host or participant account was compromised; reset credentials and revoke sessions if necessary.
- Determine whether recordings, chat, personal data, or confidential material were accessed and handle any notification duties.
- Update account-level defaults so individual hosts cannot silently disable required protections.

06 Zoombombing vs. account compromise

Zoombombing is unauthorized meeting participation. Account compromise means an attacker controls a host or attendee account and may create meetings, read invitations, or change settings. A meeting bomber can enter with a leaked link and no stolen account, but repeated or privileged incidents should trigger an account-security investigation.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com