



Zoombombing: How unwanted guests disrupt online meetings

What it is Zoombombing is unauthorized entry into a Zoom or other online meeting, usually to disrupt participants, display offensive material, record information, or harass attendees. The term became common when public meeting links and...

PUBLISHER

Gridinsoft Support

UPDATED

Jul 17, 2026

READ TIME

1 min

What it is

Zoombombing is unauthorized entry into a Zoom or other online meeting, usually to disrupt participants, display offensive material, record information, or harass attendees. The term became common when public meeting links and weak default controls allowed strangers to join large numbers of remote events.

How it works

An intruder may find a meeting link posted publicly, receive it from another person, reuse a recurring identifier, or guess details when additional controls are absent. Once admitted, permissive screen sharing, chat, microphone, file transfer, or renaming settings can amplify the

disruption.

Key points

- The problem is not limited to Zoom; any meeting platform can be disrupted when access and participant permissions are weak.
- A meeting password embedded in a publicly shared link offers little protection from people who obtain the full link.
- Recordings, participant names, and chat can create privacy or safeguarding concerns beyond the live disruption.

What to do

- Use unique meeting links, waiting rooms, authenticated attendees, and host-controlled admission for sensitive events.
- Restrict screen sharing, file transfer, recording, and unmuting until participants need them.
- Do not publish private meeting links on open websites or social posts.
- Remove and report intruders, preserve relevant logs, and issue a new meeting link after exposure.

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](https://support.gridinsoft.com)