ZOOMBOMBING: BEING PREPARED (EMPLOYEES)

What is Zoombombing?

Zoombombing is a form of trolling where hackers gain access to a Zoom meeting and attempt to disrupt the video chat by displaying or shouting profanity, racial epithets or displaying disturbing or offensive images on the video feed.

How do hackers access Zoom?

If your Zoom meeting is set to public in the privacy settings, then your zoom meeting can be accessed by anyone with the correct link. Posting the Zoom link on social media platforms also provides access to unauthorized hackers.

How to prevent Zoombombing?

Consider using one of the secure tools provided by the university, which are listed in the section below, to host virtual meetings rather than Zoom. If you do chose to use Zoom, guidelines for securing meetings are here. Some of these measures include:

1. Do not share the Zoom link publicly.
2. Install Zoom updates and lock your meeting using the security icon.
3. Set all meeting links to "Private". This is done by default by Zoom and now attendees must have a password to access.
4. Do not use your personal meeting ID. This is assigned to every registered Zoom user and does not change and with this ID, it provides access to your personal virtual meeting room.
5. To avoid zoombombing, only share your personal meeting ID with trusted contacts.
6. Enforce chat restrictions and disable whiteboarding and annotations.
7. If you believe your Zoom personal meeting ID has been compromised, contact Zoom directly to have it changed.
8. Restrict video sharing by setting the screen sharing setting to "Host only". If others need to share video during the meeting, return the setting to "Host only" when they are done.

What are some alternative virtual meeting resources?

The university offers several vetted, secure, and supported technologies for virtual meetings, including **Webex**, **Webex Teams**, and **Microsoft Teams**.

Webex is integrated into iCollege, allowing for controlled access and added security. To further secure Webex meetings, follow these guidelines on *Windows* | *Mac*.

Does Zoombombing violate university policies?

Yes. Georgia State University policies and procedures for faculty, staff, and students associated with discrimination, harassment, and sexual misconduct are applicable to zoombombing and should be followed. See section on Reporting Zoombombing.

Reporting Zoombombing

Meeting/Class Interruption
Cyber Security
help@gsu.edu
(404) 413-4357

Making formal or informal complaints of harassment, discrimination or retaliation
AA/EEO Investigations & Hiring
equalopportunity@gsu.edu
(404) 413-2561

Office of the Dean of Students
deanofstudents@gsu.edu
(404) 413-1515

Zoombombing Related Education

Harassment, Discrimination, Retaliation and Title IX
AA/EEO Training & Compliance
equitycompliance@gsu.edu
(404) 413-2567

Diversity and Inclusion
Diversity Education Planning
(404) 413-3350
diversity@gsu.edu

Student Code of Conduct and Title IX
Office of the Dean of Students
deanofstudents@gsu.edu
(404) 413-1515

Threat to Life/Safety

University Police
(404) 413-3333 or 911

Employee Assistance Program

Faculty and Staff Assistance
(404) 413-3357
fasa@gsu.edu

Sources: https://www.adl.org and https://wsu.edu/