# SUMIT

## IT SECURITY EVENT SERIES

WEEKLY IN OCTOBER

## Reimagined

INFORMATION AND
TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

Follow Along @umichTECH
Join the Coversation #SUMIT21

# Zoom Security and Privacy Updates:

## Journey since Implementation

Maggie Davidson & Asmat Noori

ITS Support Services & ITS Information Assurance

INFORMATION AND
TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

SUMIT Reimagined

# Zoombombing:

## Security in Zoom

# “Zoombombers”

- “Zoombomber” - an uninvited person who joins a video conferencing meeting or webinar, often with malicious intent to disrupt the event
- Zoombombing is illegal in the US
- Zoombombing became a global problem when the world moved to video conferencing due to the pandemic
- Zoombombing does not only impact Zoom--it impacts all video conferencing tools (named because Zoom is the most widespread tool)

# How do Zoombombers get in?

- Brute Force: randomly trying a meeting/webinar ID or URL until they find one that is in session that they can join
- Exploited Info: finding a meeting/webinar ID or URL posted on publicly accessible websites or shared with them directly
  - Posted by the organizers on U-M sites for promotion
  - Posted by a participant on social media, such as by a student who thinks it would be “funny” to have a Zoombomber interrupt class
  - Sent by a participant directly to the Zoombomber

# What might Zoombombers do?

Every situation is different, but here are some things Zoombombers might do

- Share their screen to show disturbing images or videos
- Say disturbing things or play disturbing audio
- Show disturbing images, videos, or text on their camera
- Post disturbing messages in the chat (meetings or webinars) or Q&A (webinars only)
- Change their display name to disturbing phrases

# What can I do?

1. **Proactively Control Access (“Access”)**: Prevent Zoombombers from getting in
    - It is VERY IMPORTANT that you add security settings to your meetings, webinars, and recordings
    - Avoid posting Zoom meeting, webinar, or recording URLs publicly
2. **Proactive Settings (“Settings”)**: Control what participants can do to minimize possibilities for disruption if a Zoombomber does get in
3. **Reactive**: Know how to respond if Zoombombers do get in
4.

# Access: Security Settings Comparison

| Security Setting | Effective at preventing **brute force** attacks? | Effective at preventing **exploited info** attacks? |
|---|---|---|
| Require authentication to join - University of Michigan Users | Yes | Yes |
| Passcode | Yes | No |
| Waiting Room | Yes | Yes |

# Use Webinars instead of Meetings for Public Events

- Zoom Webinars are more secure than Meetings because Zoombombers cannot do as much to disrupt the event
- Webinars give the host more control over attendees--attendees cannot be seen (video) or heard (audio) or share their screens unless the host permits it
- Reference: Zoom Best Practices for Publicly Accessible Events

# Selected updates since March 2020: Access

- *Mar/Apr 2020*: U-M created the University of Michigan Users option in Require Authentication (only U-M Zoom users can join, must log in)
- *May 2021*: All U-M Zoom meetings must be secured with a security option (Require Authentication, Waiting Room, Passcode)
- *~Feb 2021*: hosts may grant an Authentication Exception to specific users to allow them to bypass the Require Authentication setting
    - Helpful when most attendees will be U-M, but a few won't, such as guest speaker

# Selected updates since March 2020: Other

- *Mar 2020, Aug/Sep 2020, Mar 2021*: U-M education campaigns about Zoom security (emails, live trainings/recordings)
- *~Summer 2020, continued to refine since*: Zoom created the Security section of the in-meeting toolbar to allow hosts easy access to proactive and reactive security controls in the meeting
- *Aug 2020*: Default settings for new cloud recordings (host can change) set to limited to U-M Users and only the host can download

# What to do if you get Zoombombed

- Major disruption (e.g. multiple disruptors): **Suspend Participant Activities** via In-Meeting Security options
- Minor disruption: **Remove** disruptor via In-Meeting Security Options
- Email security@umich.edu and include as much info as possible (meeting/webinar URL, host uniqname, date/time, names of disruptors, nature of disruption, etc)
- Reference: How to Secure Meetings and Webinars

# Impact

- Zoombombing reports at U-M have gone down steadily over time, particularly since requiring at least one security option in May
- U-M community members have been getting better at securing their meetings and choosing the right security option for them
- New features allow meetings and webinars to be secure without sacrificing engagement and productivity

# My Zoom Data:

## Privacy in Zoom

# What can Zoom do with my data?

U-M has contracts and agreements with Zoom that specify:

- They are required to secure and protect U-M data.
- They can only use U-M data to help them run and improve their services.
- They may not sell or rent U-M data.
- U-M owns the data.

Reference: [Videoconferencing Privacy, Security, and Compliance]

# What can U-M and instructors do with my data?

- U-M admin access to your data is outlined in Privacy and the Need to Monitor and Access Records (SPG 601.11)
- Recordings (in class or virtual) where students can be identified are:
  - Regulated by the Family Educational Rights and Privacy Act (FERPA)
  - Subject to state privacy laws that prohibit or limit recording conversations without consent.
- Reference: Videoconferencing Privacy, Security, and Compliance

# Instructors’ responsibilities in recording classes

- Instructors can record class activity if they notify students (with reasonable notice and option to opt out)
- Instructors can share recordings of class activities with students in the class, but must obtain students’ written consent before sharing more broadly
- Reference: Recording Class Activities: (Some) Rules of the Road

# What controls do I have over my privacy in Zoom?

- You can choose to turn off your video in a Zoom meeting to avoid being seen
- You can choose to not speak/mute audio in a Zoom meeting to avoid being heard
- Being recorded:
  - When recording is started in any U-M Zoom meeting, all participants receive both an audio and a visual notification
  - Participants are prompted to consent to being recorded
  - Participants have the opportunity to withhold consent and instead leave the meeting; by remaining in the meeting, they are providing consent to be recorded

# Resources

- How to Secure Meetings & Webinars (U-M resource)
- Zoom Best Practices for Publicly Accessible Events (U-M resource)
- Videoconferencing Privacy, Security, and Compliance (U-M resource)
- Recording Class Activities: (Some) Rules of the Road (U-M resource)
- Protect Content and Privacy in Zoom Cloud Recordings (U-M resource)
- Zoom Trust Center (vendor information about security, privacy, etc)