DEPARTMENTAL COMPUTING SUPPORT SYMPOSIUM, FALL 2020

# Securing Zoom Meetings

Dan Yaffe and Quinn Warnick, TLOS

October 21, 2020

INFORMATION TECHNOLOGY
TECHNOLOGY-ENHANCED LEARNING
AND ONLINE STRATEGIES
VIRGINIA TECH™

# Zoom Status Report

| Month | New Users | Number of Meetings | Total # of Meeting Minutes |
|---|---|---|---|
| July | 2,587 | 76,425 | 21,445,045 |
| August | 8,897 | 88,581 | 35,897,191 |
| September | 1,919 | 152,784 | 71,846,726 |
| October (to date) | 366 | 56,558 | 23,973,962 |

**Quick Facts:**

➢ VT has 44,027 active “pro” licenses (plus 19,491 “free” licenses for alumni)

➢ September 2020 meeting minutes = 136.69 calendar years

➢ Year-over-year growth in meeting minutes: 2,910%

# Zoom Security Incidents, Fall 2020

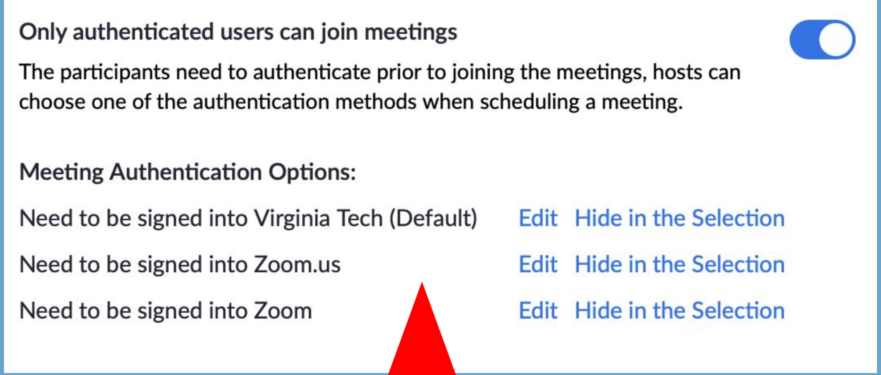
- 11 significant "Zoom bombing" incidents reported and investigated.
- Incidents can be reported by contacting 4Help, or by calling 911 directly if there is a threat to the safety of any participant.
- Process for responding to Zoom bombing incidents:
  - TLOS gathers all technical information from Zoom.
  - IT Security Office reviews Zoom logs and attempts to determine location information of bad actors.
  - Any VT students involved are referred to the Office of Student Conduct.
  - VT Police Department works with Zoom and law enforcement in other jurisdictions, if applicable.
  - TLOS provides training for individuals and groups hosting meetings that were interrupted.

# Best Practices for Securing Zoom Meetings

1. Never share meeting IDs or passcodes via social media.
2. Always use a meeting passcode or waiting room.
3. Consider restricting meeting attendance to authenticated Zoom users. (Even more restricted: authenticated Virginia Tech users.)
4. Stay signed into Zoom with your Virginia Tech account.
5. Keep the Zoom app updated to the latest version to benefit from security improvements and bug fixes.
6. Don’t use your personal meeting ID for public or recurring events.
7. Consider using meeting registration for events that need to publicized.

# Account Settings vs. Meeting Settings

- ➢ Account settings determine defaults for all meetings scheduled by a user.
- ➢ Meeting settings can override account settings on a per-meeting basis.



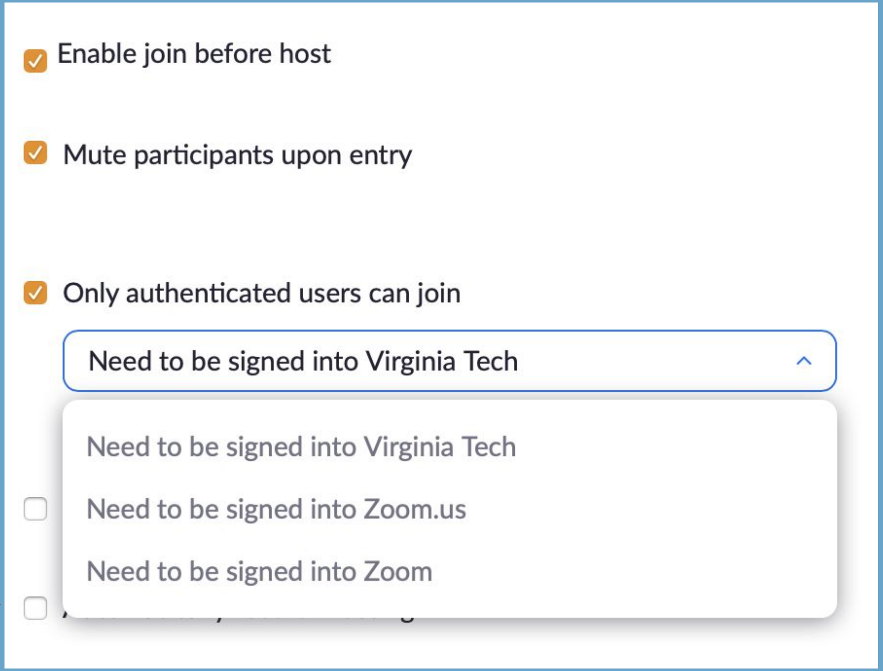
**Only authenticated users can join meetings**

The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.

**Meeting Authentication Options:**

| | | |
|---|---|---|
| Need to be signed into Virginia Tech (Default) | Edit | Hide in the Selection |
| Need to be signed into Zoom.us | Edit | Hide in the Selection |
| Need to be signed into Zoom | Edit | Hide in the Selection |

**Account Settings**



☑ Enable join before host

☑ Mute participants upon entry

☑ Only authenticated users can join

Need to be signed into Virginia Tech ^

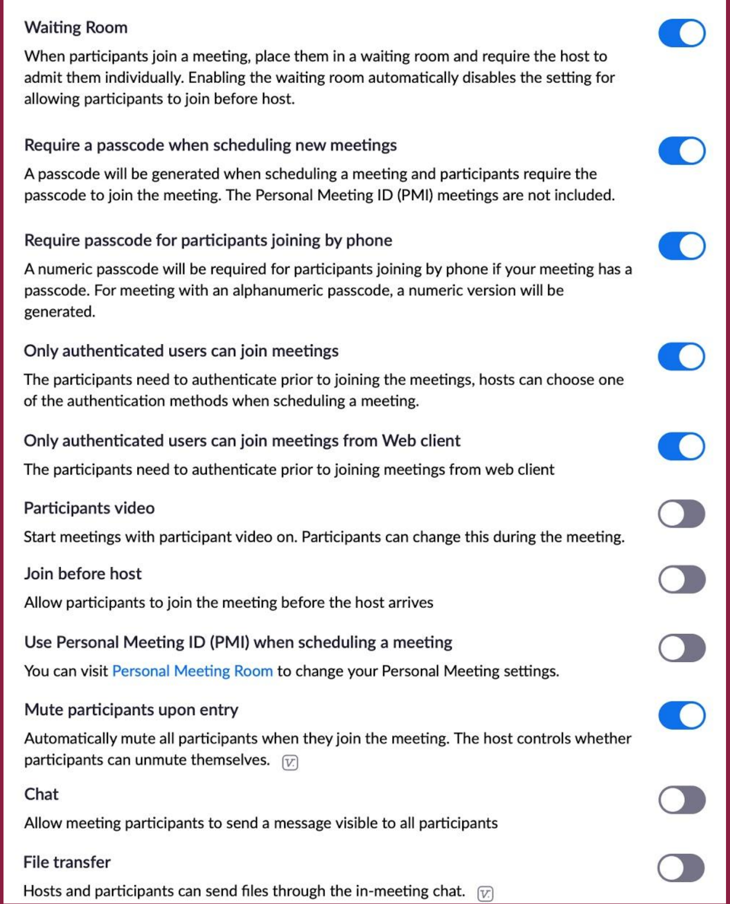
- Need to be signed into Virginia Tech
- Need to be signed into Zoom.us
- Need to be signed into Zoom

☐

☐

**Meeting Settings**

# Most Aggressive Security Settings



**Waiting Room** ☑
When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

**Require a passcode when scheduling new meetings** ☑
A passcode will be generated when scheduling a meeting and participants require the passcode to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

**Require passcode for participants joining by phone** ☑
A numeric passcode will be required for participants joining by phone if your meeting has a passcode. For meeting with an alphanumeric passcode, a numeric version will be generated.

**Only authenticated users can join meetings** ☑
The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.

**Only authenticated users can join meetings from Web client** ☑
The participants need to authenticate prior to joining meetings from web client

**Participants video** ☐
Start meetings with participant video on. Participants can change this during the meeting.

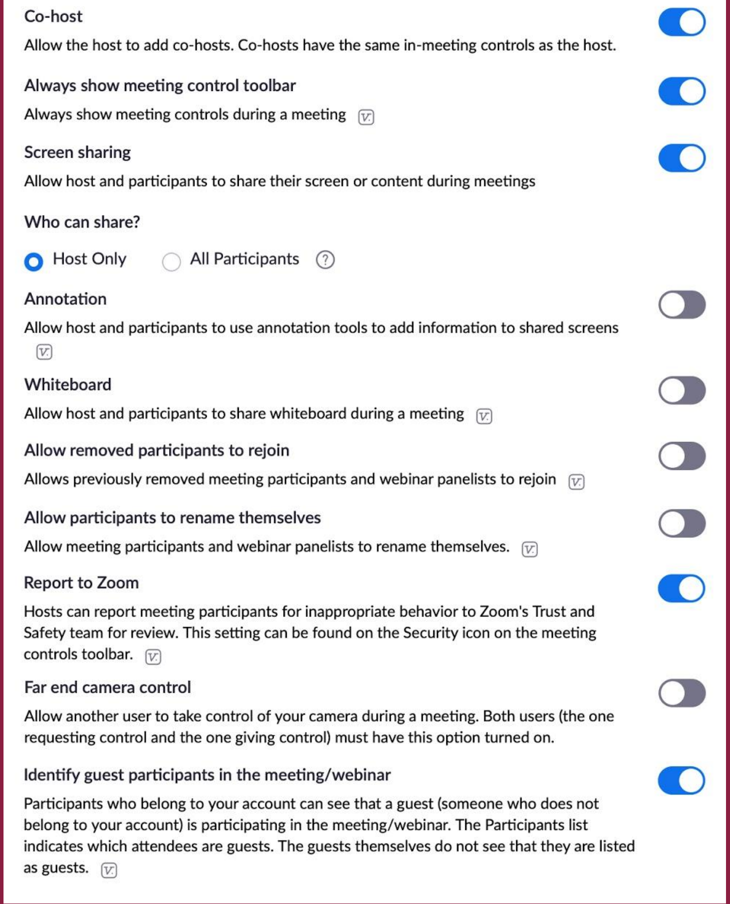
**Join before host** ☐
Allow participants to join the meeting before the host arrives

**Use Personal Meeting ID (PMI) when scheduling a meeting** ☐
You can visit Personal Meeting Room to change your Personal Meeting settings.

**Mute participants upon entry** ☑
Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.

**Chat** ☐
Allow meeting participants to send a message visible to all participants

**File transfer** ☐
Hosts and participants can send files through the in-meeting chat.



**Co-host** ☑
Allow the host to add co-hosts. Co-hosts have the same in-meeting controls as the host.

**Always show meeting control toolbar** ☑
Always show meeting controls during a meeting

**Screen sharing** ☑
Allow host and participants to share their screen or content during meetings

Who can share?

● Host Only ○ All Participants

**Annotation** ☐
Allow host and participants to use annotation tools to add information to shared screens

**Whiteboard** ☐
Allow host and participants to share whiteboard during a meeting

**Allow removed participants to rejoin** ☐
Allows previously removed meeting participants and webinar panelists to rejoin

**Allow participants to rename themselves** ☐
Allow meeting participants and webinar panelists to rename themselves.

**Report to Zoom** ☑
Hosts can report meeting participants for inappropriate behavior to Zoom's Trust and Safety team for review. This setting can be found on the Security icon on the meeting controls toolbar.

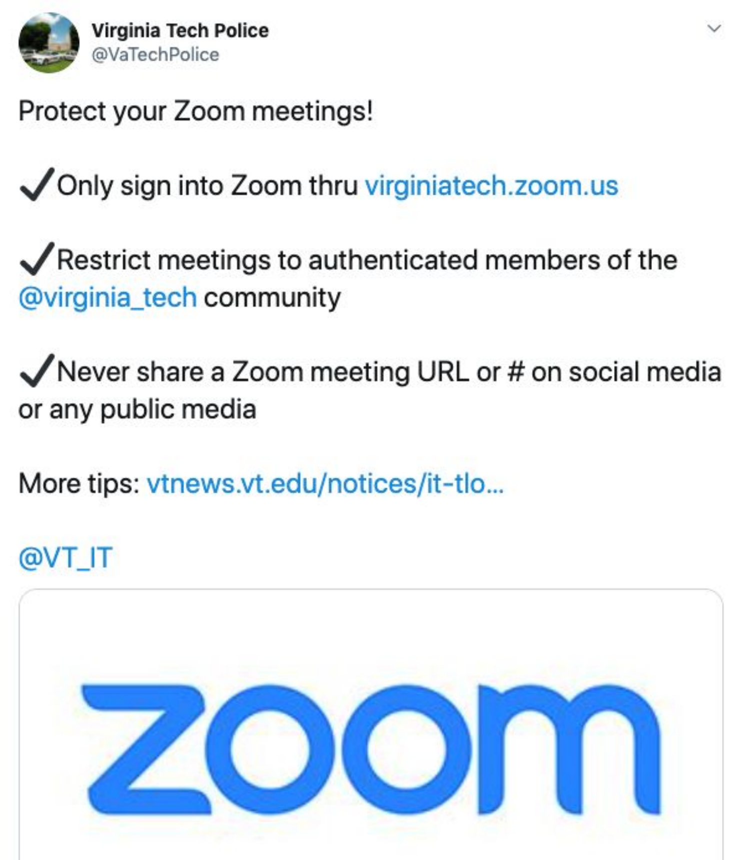
**Far end camera control** ☐
Allow another user to take control of your camera during a meeting. Both users (the one requesting control and the one giving control) must have this option turned on.

**Identify guest participants in the meeting/webinar** ☑
Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests. The guests themselves do not see that they are listed as guests.

# Responding to Zoom Bombing in the Moment

- Most Zoom bombing attacks are carried out by groups of bad actors working together, not by single individuals. It is likely they are coordinating the attack in another venue and have multiple strategies for disrupting the meeting.
- Once a Zoom bombing incident begins, it is very difficult to remove every attacker and regain control of the meeting.
- **Recommendation:** As soon as the host becomes aware that a Zoom bombing incident is in progress, they should immediately end the meeting for all participants.
- If the community has a safe "second location" where legitimate meeting participants can regroup (e.g., Slack, Google Group), the host can direct them to that space, where new meeting information can be shared privately.

# VT's Proactive Measures for Reducing Zoom Attacks



**Virginia Tech Police**
@VaTechPolice

Protect your Zoom meetings!

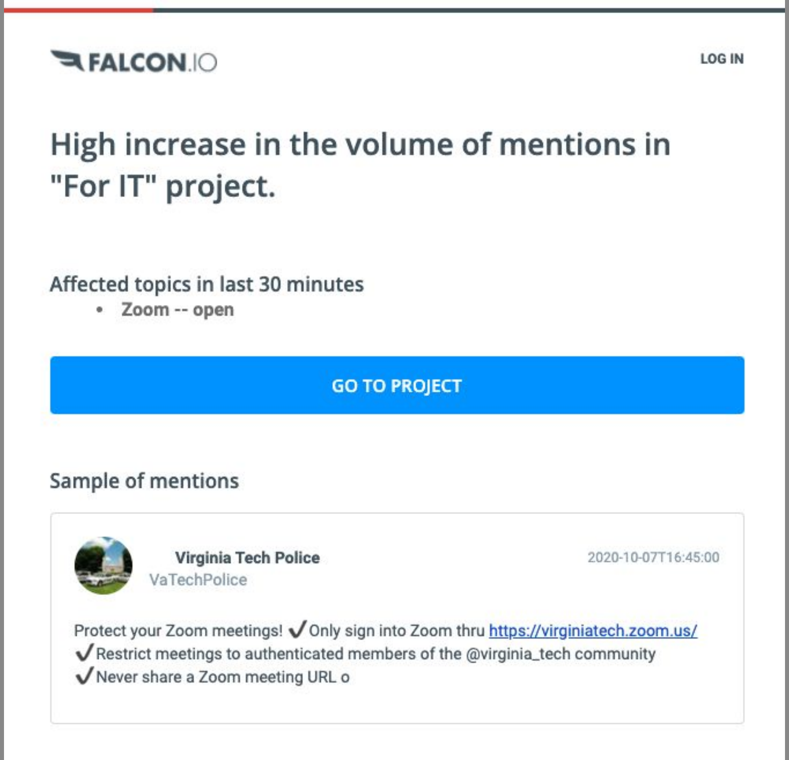
✓Only sign into Zoom thru virginiatech.zoom.us

✓Restrict meetings to authenticated members of the @virginia_tech community

✓Never share a Zoom meeting URL or # on social media or any public media

More tips: vtnews.vt.edu/notices/it-tlo...

@VT_IT



High increase in the volume of mentions in "For IT" project.

Affected topics in last 30 minutes

- Zoom -- open

Sample of mentions

**Virginia Tech Police** 2020-10-07T16:45:00
VaTechPolice

Protect your Zoom meetings! ✓Only sign into Zoom thru https://virginiatech.zoom.us/
✓Restrict meetings to authenticated members of the @virginia_tech community
✓Never share a Zoom meeting URL o

# Coming Soon at Virginia Tech...

- TLOS plans to enable “Only authenticated users can join meetings” by default. We encourage all users to leave this turned on, but individuals can disable this in their account or meeting settings.
- To enhance meeting security, all of Virginia Tech’s Zoom meetings will require one (or more) of the following:
  - Meeting passcode
  - Waiting room
  - Restrict attendance to authenticated users
- Additional information will be communicated to the campus community prior any changes being implemented.

# We Need Your Help!

- Zoom Rooms for classrooms, conference rooms, etc., need to be kept updated to the latest version of the software. (Please remember to update both the computer running Zoom Rooms software and the tablet controller.)
- If you need add-on services or features from Zoom, please contact TLOS so we can purchase these items using our institutional contract: tlos@vt.edu
- Please teach and model best practices in your own meetings and in your conversations with faculty, students, and IT colleagues.

# Additional Resources

- ➢ Zoom: “Best Practices for Securing Your Zoom Meetings”
- ➢ Zoom: “Best Practices for Securing Your Virtual Classroom”
- ➢ Zoom: “How to Keep Uninvited Guests Out of Your Zoom Event”
- ➢ TLOS: “Best Practices to Secure Zoom Meetings”
- ➢ 4Help Knowledge Base: “Best Practices for Security”

# Questions? Feedback?

Thanks for listening.

Let’s keep talking:

**tlos@vt.edu**

INFORMATION TECHNOLOGY
TECHNOLOGY-ENHANCED LEARNING
AND ONLINE STRATEGIES
VIRGINIA TECH™