To the Kellogg Community -

I'm writing this to address what happened last week at our Kellogg PTSA Board and Membership Zoom meeting on 9/24. To put it in a nutshell — we got "zoom bombed" about 11 minutes into the PTSA presentation. Below is an account of what happened:
- We posted a FB and Instagram meeting invitation (now deleted) that contained a link to the zoom meeting.
- We had approximately 30 people in the waiting room.
- We were running a few minutes late, and the co-hosts admitted all attendees at once.
- At around 11 minutes into the meeting, the "attacker(s)" hijacked the meeting by posting:
  – derogatory and hate speech
  – showing an emoji on the host's screen and voice-over or live speaking to only the host saying, "This is not a curse, Consider this a Blessing."
- We terminated the zoom meeting so that the attackers could not continue.
- After some time, we restarted a Zoom meeting and only admitted those verified by the host.
- From that point, we had no other attacks and were able to complete our meeting.
- Sadly, we did lose more than a handful of attendees once we all logged back on.

This type of attack has been mentioned in the news media in the past months and has become more prevalent because of Zoom's high usage as an online meeting tool.

We believe the attackers discovered our Kellogg community Zoom meeting URL (most likely via FB or Instagram), allowing them to gatecrash our meeting. Zoom has several collaborative features that are turned on by default that we were not aware of, which also opened us up to this type of an attack.

After the call, I immediately spoke with the Secretary and Co-President of the PTSA Board to discuss what happened and what to do next time. I also researched and reached out to the Shoreline PTA Council to create best practices for future Zoom meetings to include guidance on setting up a public meeting to prevent Zoom bombing attacks.

Reaction
I can't begin to describe how traumatizing this experience was — to see our members and community victimized in what should have been a secure and safe space for us to conduct our community meeting.

Some special thanks are in order:
- To our executive board leadership for handling the meeting with immediacy and composure.
- To Amy Reed, who was on our call and able to give us the notification of what was happening and instant guidance
- To all our attendees for being so supportive and coming back to the meeting!

My message to all of you is how incredibly sorry this incident occurred. These sorts of racist attacks are harmful to us all, especially our community members of color, and we deeply

apologize for any impacts this has left. We will continue to work hard to create safe spaces for future PTSA membership meetings.

I've put some more information below on how these attacks work, what we've learned and some of the measures we will take to safeguard ourselves.

Last, thanks for your messages of support to our team and your understanding. If you have ideas, suggestions, or feedback, please feel free to email me directly at president@kelloggptsa.org.

Myrna Habermann
Kellogg PTSA President

How the zoom attack works:
- Zoom "meetings" (as opposed to "webinars") allow for any attendee to turn on camera and mic
- Attackers can cycle through random numbers looking for an active meeting.
- The attackers can also find zoom meeting URLs posted on social media (this may be our case)
- Zoom hackers take advantage of the collaborative settings that are set by default

What we learned:
- If your meeting is attacked, terminate the session immediately (don't try to block attackers).
- Have an instant-message back channel with your speakers in case something goes wrong
- Communicate with attendees as soon as you can
- Contact Zoom immediately
- Don't give up!

What we're changing:
- All zoom meetings will be password protected
- We may apply additional restrictions to who can post chat messages/share video/audio in a meeting
- We may apply conditions only to allow registered attendees to join meetings
- The PTSA will contemplate evaluating other forms of meeting/webinar software other than Zoom, the reason being:
  - Contacting technical support resulted in canned auto-responses
  - Contacting Zoom support by phone to report the attack and initiate an investigation resulted in being on hold for over an hour. After my report, they said: "we'll contact you" - it's now been a week plus with no return communication.