March 21, 2022

Supporting Our Community with Zoom Security Measures

Dear Colleagues,

Colleges across the country have been experiencing a surge of attacks on Zoom meetings, and Baruch College is no exception. By finding new ways to adapt methods to avoid detection, attackers have begun to use social media to share meeting information along with tactics that have resulted in a greater burden of preparation, vigilance, and use of security measures being placed on meeting hosts and attendees.

I avoid using the term “Zoombombing,” because it risks understating the severity of these incidents, which do not involve the type of playful gestures and prankish intent that we associate with photobombing. These incidents are not pranks; rather, they are vicious attacks that are designed to frighten and demean meeting attendees by using offensive language and displaying graphic images. The experience is not easily forgotten, and I regret that members of the Baruch community have had this unfortunate experience.

Please take the time to review the Zoom security measures that the Center for Teaching and Learning has included in its guide to Teaching with Zoom and the safety tips offered by the Office of Student Life. Both of these reference tools detail the University’s Zoom Security Protocol that we should all be following.

I cannot list all of the security measures here but would like to highlight a few essential points:

- Do not post meeting codes on public sites.
- Use authentication whenever possible. For this to be effective, the Baruch community has to become accustomed to logging into the Zoom client with our CUNY Login credentials (firstname.lastname##@login.cuny.edu) before clicking
on a link to a meeting. This practice adds a step to the process, but it is worth the effort.

- Include a waiting room and passcode in your personal meeting room settings.
- Hosts should be prepared to use the Zoom functions that Suspend Participant Activities and Remove Participants from a meeting. This can be a challenge, because the initial reaction to the attack may be shock, which is what the attackers hope.

BCTC staff can assist you with understanding how to use Zoom security measures after you have read through the resources cited above. To schedule a consultation, send an email message to the Help Desk with the subject line “Zoom security.”

Let’s take the steps that are necessary as meeting hosts and attendees to support one another in the Baruch community from Zoom attacks. Thank you.

Sincerely,

Arthur Downing, PhD
Vice President for Information Services and Dean of the Library