April 6th, 2020

BRIEFING NOTE AND PROTOCOLS FOR ZOOM BOMBING

There have recently been concerns regarding "Zoom Bombings." A Zoom bombing is when a hacker or hackers gain access to a Zoom meeting and attempts to disrupt the video and/or chat box and upset participants by shouting profanity or putting graphic images in their video feed.

IMPACT wishes to reassure our Members that we are aware of the situation and are working to minimize the risk of this happening to any of the meetings or training sessions we host and would like to share the following best practices with IMPACT members.

IT experts are recommending that all organizations implement the following security measures including:

- All virtual training sessions require registration through Eventbrite or another platform to receive Zoom session information
- All meeting rooms for virtual sessions should be private and participants require a password to enter the room
- All meetings and virtual training sessions should be held in randomly generated Zoom meeting rooms rather than personal meeting rooms
- Virtual training sessions should have restricted participant capabilities. Only hosts and presenters should have the ability to share their video and screen and use their microphones.
- Links to already scheduled meetings should be updated in existing Outlook calendar invites to include the updated Zoom meeting information
- Meeting hosts are prepared with a clear and established protocol on how to manage the situation if the meeting or virtual training sessions are "bombed". Procedures can include:
    - Remove someone or put them on hold
        - If a hacker or unwanted attendee manages to slip through your established barriers, as the meeting host, you do have the power to remove someone from a call or put them on hold
            - To permanently remove someone from the meeting: During the call, go to the participants panel on the right. Hover over the name of the person you want to remove from the meeting and when options appear, choose Remove. This will remove them from the meeting and prevent them from returning.
            - To put someone on hold: During the call, find the video thumbnail of the person you want to put on hold. Click on their video image and select Start Attendee on Hold.

    - To disable an attendee's camera: Hosts can turn off any participant's camera. If someone is being rude or inappropriate on video, or their video has some technical problem, the host can open the Participants panel and click on the video camera icon next to the person's name and turn it off.

- Prevent Animated GIFs and Other Files in the Chat: In the chat area of a Zoom meeting, participants can share files, including images and animated GIFs—if the host of the meeting allows them. If you'd rather not allow your attendees use this feature, then be sure to disable file transfer. It's on by default, so you need to disable it. This must be done through the Advanced Features in your Zoom settings.

We continue to monitor this evolving situation and will update our precautionary measures and responses as new information becomes available. If you require further information on "Zoom Bombings" and how to protect yourself or your organization, *Zoom* recommends users read this detailed guide, which covers precautions for keeping their meetings safe.

If you have any questions or concerns, please contact brielle@sagese.org