Zoom Security Tips Developed by PSEA:

- DO ensure you have a unique, long, complex passphrase for the account assigned to you
  - At least 16 characters
  - Spaces and punctation work for complexity and help with the length of the passphrase

- DO create a Waiting Room for attendees. Only let in those you recognize/approve.

- DO require the host to be present on a meeting before it starts. This prohibits attendees from joining before you are ready.

- DO expel an uninvited/unintended participant as appropriate for your discussion topic.

- DO lock a meeting after all participants have entered.

- DO limit screen sharing to "host only" for meetings as appropriate, this will eliminate zoom-bombing

- DO temporarily pause screen-sharing when opening a new window to move between applications/browser windows. This avoids unintended sharing of other materials on your computer.

- DO require a password on meetings of confidential/sensitive information.

- DO ask attendees to mute themselves unless they are speaking. This will help eliminate background noise and distractions.

- DO NOT make your Zoom password the same as your network/login password!

- DO NOT have those invited share the link with others. Have them contact you to add the additional person(s) to the meeting request. This prevents unintended participants and protects against a meeting possibly being hijacked.

- DO NOT permit participants to record the meeting. As host, you can record the meeting if necessary and post later for access.
  - DO check with Customer Service as to the appropriate recording location

- DO NOT send a meeting password in the same email/email chain as the URL for the meeting. Send separately, with a new email Subject line or communicate vial phone/text if possible.