BLUE BAY TECHNOLOGY

Zoom Security

10 Steps to Take NOW

1. Password protect your meetings.
Passwords can be set at the individual meeting, user, group, or account level for all sessions. All participants require the password to join the meeting.

2. Authenticate users.
When creating a new event allow only signed-in users to participate.

3. Don't join before host.
Do not allow others to join a meeting before the host has arrived.

4. Lock down your meeting.
Lock the meeting once every expected participant has arrived. This will prevent others from joining even if meeting IDs or access details have been leaked.

5. Turn off participant screen sharing.
No one wants to see offensive material shared by a Zoom bomber. Disable the ability for meeting attendees to share their screens.

6. Use a randomly generated ID.
Choose a randomly generated ID for meetings when creating a new event. Attackers that know your personal meeting ID could disrupt online sessions.

7. Use waiting rooms.
The waiting room feature is a way to screen participants before they are allowed to enter a meeting. While legitimately useful for purposes including interviews or virtual office hours, this also gives hosts greater control over session security.

8. Avoid file sharing.
Share material using a trusted service such as Box or Google Drive instead of the file-sharing feature of Zoom meetings.

9. Remove nuisance attendees.
If someone is disrupting a meeting you can kick them out under the “Participants” tab.

10. Check for updates.
As security issues crop up and patches are deployed or functions are disabled, make sure you have the latest build.