

## **Zoom Security Developments**

- Many agencies have banned employees from using the software until Zoom's security posture improves.
- Zoom has reacted quickly but new vulnerabilities continue to be identified.
- To try and prevent Zoom-bombing -- the hijacking of meetings and a practice the US Department of Justice recently deemed a crime -- meeting ID numbers are no longer being shown in address bars (URLs).
- A dedicated security tab has been introduced to streamline the process of changing security settings for hosts and meeting attendees.
- Zoom has promised an upcoming change to where data is stored. Starting April 18, paid subscribers can opt in or out of specific data center regions.

## **Tips and Best Practices**

### 1. Password protect your meetings

The simplest way to prevent unwanted attendees and hijacking is to set a password for your meeting. Passwords can be set at the individual meeting, user, group, or account level for all sessions. In order to do so, first sign in with your account at the Zoom web portal. If you want to set up a password at the individual meeting level, head straight over to the "Settings" tab and enable "Require a password when scheduling new meetings," which will ensure a password will be generated when a meeting is scheduled. All participants require the password to join the meeting.

### 2. Authenticate users

When creating a new event, you should choose to only allow signed-in users to participate.

### 3. Join before host

Do not allow others to join a meeting before you, as the host, have arrived. You can enforce this setting for a group under "Account Settings."

### 4. Lock down your meeting

Once a session has begun, head over to the "Manage Participants" tab, click "More," and choose to "lock" your meeting as soon as 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 pornographic material shared by a Zoom bomber, and so disabling the ability for meeting attendees to share their screens is worthwhile. This option can be accessed from the new "Security" tab in active sessions.

#### 6. Use a randomly-generated meeting ID

You should avoid using your personal meeting room/ID if possible, as this could pave the way for pranksters or attackers that know it to disrupt online sessions. Instead, choose a randomly generated ID for meetings when creating a new event. In addition, you should not share your personal ID publicly.

#### 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

Be careful with the file-sharing feature of meetings, especially if users that you don't recognize are sending content across, as it may be malicious. Instead, share material using a trusted service such as Box or Google Drive.

#### 9. Remove nuisance attendees

If you find that someone is disrupting a meeting, you can kick them out under the "Participants" tab. Hover over the name, click "More," and remove them. You can also make sure they cannot rejoin by disabling "Allow Removed Participants to Rejoin" under the "Settings: Meetings - Basic" tab.

#### 10. Check for updates

As security issues crop up and patches are deployed or functions are disabled, you should make sure you have the latest build. In order to check, open the desktop application, click on your profile in the top-right, and select "Check for updates."