



Enhanced Security Features in Zoom Meetings

Dear Synechronites,

There have been several media reports about security concerns in Zoom Meetings app. Synechron IT Team has reached out Zoom and has received clarifications about enhanced security features in their latest versions. We urge you to update your Zoom desktop and mobile applications to latest version (Ver 4.6.11 or later) to ensure safe usage of the application with the help of these security features.

Synechron has been sending several tips to secure Zoom meetings from time to time. Please find below few more tips to secure your Zoom meetings.



Don't use Personal Meeting ID for Public Meetings

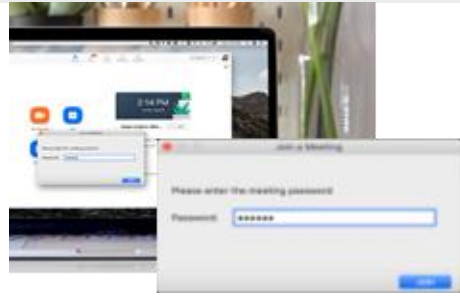
Your Personal Meeting ID (PMI) is the default that launches when you start an ad-hoc meeting.

For public meetings, you should always schedule new meetings with randomly generated meeting IDs. That way, only invited attendees will know how to join your meetings. You can also turn off your PMI before starting an instant meeting in your profile settings.

Using Mandatory Passwords

You can take meeting security even further by making it mandatory to key-in a password to join your meetings.

This feature can be applied to both your Personal Meeting ID and randomly generated meeting IDs, so only those with the password will be able to reach you, and join the newly scheduled meetings.



Please feel free to reach out to IT team should you need any help. We hope that you will make the best of Zoom by following these best practices to make your meetings secure. We shall come back with more tips to help you explore and employ Zoom optimally.

**Regards,
Team IT**

For any queries and concerns write to IT-feedback@synechron.com