

Press Information Bureau

Government of India

MHA issues Advisory on Secure use of ZOOM Meeting Platform

New Delhi, April 16, 2020

The Cyber Coordination Centre (CyCoord), under the Union Ministry of Home Affairs (MHA), has issued an advisory on secure use of ZOOM Meeting Platform by private individuals. This advisory states that the platform is not for use by Government officers/officials for official purposes.

The document makes reference to earlier advisories of the Indian Computer Emergency Response Team (Cert-In) and states that Zoom is not a safe platform. The guidelines have been issued to safeguard private individuals who would still like to use the platform for private purposes.

The broad objective of this advisory is to prevent any unauthorized entry into a Zoom Conference Room and prevent the unauthorized participant to carry out malicious attacks on the terminals of other users in the conference.

The details of protective measures to be taken by individuals may be accessed at the document attached at this link.

VG/SNC/VM


Endt. No. DA1/14532/2017/HRD

dated 22.04.2020

1. Copy Communicated to all Heads of Institutions under IHRD for strict compliance
2. I. T. Division
3. S.F
4. O.C

Sd/-
DIRECTOR

Approved for issue


Senior Superintendent

dated April 12, 2020

Advisory on Secure use of Zoom meeting platform by private individuals (not for use by government offices/officials for official purpose)

Zoom is not a safe platform and advisory of cert-in on the same dated Feb 06, 2020 and March 30, 2020 may kindly be referred. These advisories are available on Cert-In website.

2. Those private individuals who still would like to use Zoom for private purpose may kindly follow the following guidelines.

3. Broad objective of this document is to enable/disable certain settings is to .

- prevent unauthorised entry in the conference room
- prevent an authorised participant to carry out malicious on the terminals of other in the conference.
- Avoid DOS attack by restricting users through passwords and access grant

4. Most of the settings can be done by login into users zoom account at website, or installed application at PC/Laptop/Phone and also during conduct of conference. However certain settings are possible through certain mode/channel only. For example, **lock meeting** can be enabled by administrator only when the meeting has started. This documents explains in details all the security configuration through website, App and through console during the conduct of conference

Objective of security configurations:

1. **Setting new user ID and password for each meeting**
2. **Enabling *waiting Room***, so that every user can enter only when host conducting meeting admits him
3. **Disabling *join before host***
4. Allowing ***Screen Sharing* by host Only**
5. Disabling "***Allow removed participants to re-join***"
6. **Restricting/disabling *file transfer* option** (if not required)
7. ***Locking meeting*** once all attendees have joined
8. Restricting the recording feature
9. To end meeting (and not just leave, if you are administrator)