Zoom- Not a Safe Platform: MHA

drishtiias.com/printpdf/zoom-not-a-safe-platform-mha

Why in News

Recently, the **Ministry of Home Affairs** (MHA) has issued an advisory that **Zoom video conference** is not a safe platform.

> The **Indian Cyber Crime Coordination Centre (I4C)** of the MHA issued a set of guidelines for the safe usage of Zoom by private individuals.

Key Points

- Zoom has seen an **exponential rise in usage in India** as office-goers remain at home due to the **lockdown**, imposed to curb the **Covid-19** pandemic.
  - Over 90,000 schools across 20 countries have started using it regularly.
  - The **maximum number of daily meeting participants** of approximately 10 million at the end of December 2019 **grew to more than 200 million daily** meeting participants in March.
  - It has been used extensively by everyone **including the central and state ministers** for official purposes and conducting meetings.
- Zoom is a **US-based video communication and videoconferencing platform.**
  - This **Silicon Valley-based company** appears to own three companies in China through which at least 700 employees were paid to develop Zoom's software.
  - This **arrangement is apparently an effort at labor arbitrage** in which Zoom can avoid paying US wages while selling to US customers, thus **increasing their profit margin.**
  - However, this arrangement may make Zoom **responsive to pressure from Chinese authorities.**
  - Reportedly, **few calls made through the app are routed through servers in China.**

- Earlier, the **Computer Emergency Response Team, India** **(CERT-In)** had also issued advisories cautioning on the use of Zoom for office meetings.
    - It **warned that the insecure usage of the platform** may allow **cyber criminals to access sensitive information** such as meeting details and conversations giving rise to **cyber frauds.**
    - It also **highlighted multiple vulnerabilities** which could allow an attacker to gain elevated privileges or obtain sensitive information.
- **Citizen Lab,** based at the **University of Toronto,** found **significant weakness in Zoom's encryption** that protects meetings.
    - It identified the **transmission of meeting encryption keys through China.**
    - The lab has **raised two primary concerns- geo-fencing and meeting encryption.**
- **Zoom Founder and CEO Eric S Yuan** has apologised and assured the people that the **privacy and security expectations would be taken care** of.
    - Zoom has **added additional features** such as **placing a new security icon** in the meeting controls, **changing Zoom's default settings** and **enhancing meeting password complexity,** among others.
    - It has also added that soon, **account admins will have the ability to choose** whether or not their data is routed through specific data center regions.
- **Suggestions by the Ministry**
    - The users are suggested to **set strong passwords** and **enable "waiting room" features** so that call managers could have better control over the participants.
    - Users should also **avoid using personal meeting ID** to host events and instead **use randomly generated meeting IDs** for each event.
    - People using the app **should not share meeting links on public platforms.**

Indian Cyber Crime Coordination Centre

- The scheme to set up I4C was **approved in October 2018,** to **deal with all types of cybercrimes in a comprehensive and coordinated manner.**
- It has **seven components:**
    - National Cyber Crime Threat Analytics Unit
    - National Cyber Crime Reporting Portal
    - National Cyber Crime Training Centre
    - Cyber Crime Ecosystem Management Unit
    - National Cyber Crime Research and Innovation Centre
    - National Cyber Crime Forensic Laboratory Ecosystem
    - Platform for Joint Cyber Crime Investigation Team.
- Various States and Union Territories (UTs) have consented to set up **Regional Cyber Crime Coordination Centres.**
- This **state-of-the-art** Centre is located in **New Delhi.**

Computer Emergency Response Team-India

- It is an organisation of the **Ministry of Electronics and Information Technology,** Government of India, with the **objective of securing Indian cyberspace.**
- It is the **nodal agency** which deals with **cybersecurity threats like hacking and phishing.**
- It collects, analyses and disseminates information on cyber incidents, and also issues alerts on cybersecurity incidents.
- CERT-IN provides **Incident Prevention and Response Services** as well as **Security Quality Management Services.**

Source: TH